

ORIGINAL RESEARCH ARTICLE

Cybersecurity Vulnerabilities and Data Privacy in Modern Healthcare Systems: A Systematic Review

Parhlad Singh Ahluwalia^{1*}¹ Dr. Bhim Rao Ambedkar Law University, Jaipur, Rajasthan, India*Corresponding Author: Parhlad Singh Ahluwalia | Email: ahluwalia002@zohomail.in | ORCID: [0000-0002-6086-8616](https://orcid.org/0000-0002-6086-8616)

ABSTRACT

Background: Healthcare has become one of the most heavily digitised and most frequently attacked sectors. Electronic records, connected medical devices, telemedicine platforms and artificial intelligence (AI) now depend on a large and often fragile digital infrastructure.

Objective: This review identifies, compares and critically analyses the cybersecurity vulnerabilities and data-privacy risks reported for modern healthcare systems. It also evaluates the technical, organisational, legal and equity-related responses proposed in the literature.

Methods: A review protocol was developed following the PRISMA 2020 statement. Eligibility criteria, information sources, selection, data extraction and synthesis are reported in Table 1. Findings were integrated through an analytical thematic synthesis and compared across earlier reviews and across regulatory regimes.

Results: Seven interlocking themes emerged: (i) a threat landscape dominated by ransomware, phishing and insider error; (ii) weak security in connected devices and smart environments; (iii) the limits of de-identification and the promise of privacy-enhancing technologies; (iv) organisational and leadership failures; (v) inequity and stigma as privacy harms; (vi) fragmented legal frameworks; and (vii) systemic resilience, including supply chains, remote work and infrastructure.

Conclusion: Healthcare security is a patient-safety problem and not only an information-technology problem. Technical controls fail without governance, workforce capacity and legal clarity. Privacy harms fall unevenly on vulnerable populations. A layered, equity-aware and leadership-driven model of "security by design" is proposed.

Keywords: *healthcare cybersecurity; data privacy; ransomware; electronic health records; medical devices; PRISMA; health data governance*

1. INTRODUCTION

Healthcare delivery is being reorganised around data. Hospital management, diagnostics, patient engagement and remote care have all moved onto digital platforms. Recent syntheses describe the effects of digital transformation on hospital management [1], the growing role of AI in diagnostic medicine [2], the redesign of patient engagement in AI-driven systems [3], and the uneven access to telemedicine across socioeconomic groups [4]. These developments promise faster diagnosis, wider access and lower cost. They also enlarge the attack surface of institutions whose core mission is the preservation of human life.

The security problem is old but intensifying. An early and influential commentary asked bluntly how safe healthcare systems really were, and answered that clinical and administrative networks had grown faster than the security practices protecting them [5]. A systematic review of modern threats and trends reached a similar conclusion. It found that the sector faces a wide mix of malicious software, social engineering, insider misuse and technical failure, with comparatively little empirical evidence about which defences work [6]. Over the period 2010 to 2017, a national analysis of reportable breaches in the United States found that breaches were recurrent, large in scale and not declining [7]. Industry cost surveys have consistently ranked healthcare among the most expensive sectors for a data breach, with average losses above ten million United States dollars in recent editions [8].

The consequences go beyond financial loss. The 2017 WannaCry ransomware outbreak disrupted large parts of the National Health Service in England. A retrospective impact analysis reported cancelled appointments, diverted emergency care and substantial recovery costs [9]. Commentators in the medical literature recognised early that such events were public-health threats and not merely IT failures [10]. Later work documented a sustained rise in ransomware attacks against healthcare delivery organisations [11]. Ransomware attacks on one hospital have been shown to strain neighbouring emergency departments [12]. Breach remediation has also been associated with measurable changes in hospital quality indicators [13]. Cyber-attacks therefore act as clinical events, because they alter waiting times, treatment pathways and outcomes.

Governance and institutional behaviour are central to this picture. Research on healthcare leadership argues that management style and administrative culture shape how organisations prepare for and respond to disruption [14], and organisational learning from pandemic failures offers lessons directly relevant to cyber-crisis response [15]. A parallel strand of scholarship situates health data within wider debates about state power. It examines how digital surveillance and techno-authoritarian practice affect sovereignty and rights in the Global South [16], and how states weaponise the internet in geopolitical conflict [17]. Health data are therefore both clinical records and strategic assets, which raises the stakes of every vulnerability.

Several reviews have mapped parts of this terrain. Early work examined security and privacy in electronic health records [18]. Narrative reviews have described trends, threats and ways forward [19]. Organisational perspectives have analysed hospital security as a socio-technical system [20]. Other authors have discussed hospital cybersecurity challenges and mitigation [21], summarised breach insights and implications [22], and reviewed cyber risk in health facilities [23], hospital risks and gaps for non-specialists [24], and capability in Australian healthcare organisations [25]. These reviews differ in scope, method and period, and they often treat technical, organisational and legal questions in isolation. Few interrogate how privacy harms interact with inequity, or how the conclusions of different reviews compare when placed side by side.

This review addresses that gap. Its objectives are to:

- identify the principal cybersecurity vulnerabilities and privacy risks reported in modern healthcare systems;
- compare the findings, methods and limits of earlier reviews;
- analyse the problem from technical, organisational, legal and equity perspectives; and
- derive an evidence-informed framework to guide policy and practice.

2. Conceptual and Regulatory Background

2.1 Security, privacy and the particular nature of health data

Information security is conventionally described through three properties: confidentiality, integrity and availability. Standard frameworks for managing cyber risk organise controls around identifying, protecting, detecting, responding to and recovering from incidents [26]. In healthcare each property has a clinical meaning. A loss of confidentiality exposes diagnoses, genetic information and mental-health history. A loss of integrity may alter a medication dose or a laboratory value. A loss of availability can delay surgery, disable monitoring equipment or force ambulance diversion. Availability and integrity attacks can therefore harm patients directly, a feature that distinguishes healthcare from most other critical sectors.

Privacy is related to security but not identical to it. Security protects systems against unauthorised access. Privacy concerns whether information about a person is collected, used, shared and retained in ways the person would reasonably expect and has consented to. A hospital can be perfectly secure and still violate privacy by sharing records lawfully but inappropriately, and an insecure system can be privacy-respecting in design but exposed in practice. Health data also have unusual properties. They are permanent, because a diagnosis cannot be reissued like a stolen password. They are relational, because genetic information reveals facts about relatives. They are stigmatising, because disease labels can invite discrimination, as work on cancer-related stigma among students illustrates [58]. They are also commercially valuable, because they can feed identity fraud, insurance manipulation and research markets.

2.2 Legal architecture

Legal protection of health data is fragmented across jurisdictions. The European Union treats data concerning health as a special category requiring heightened protection under its General Data Protection Regulation (GDPR)

[27]. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) and its Privacy, Security and Breach Notification Rules govern covered entities and their business associates [28]. India enacted the Digital Personal Data Protection Act in 2023, which establishes a consent-based regime built on the concept of data fiduciaries and a dedicated enforcement board [29]. At the international level, the World Health Organization's global strategy on digital health encourages countries to build trusted and secure digital health ecosystems [30]. Section 6 compares these regimes in detail.

2.3 Patient safety as the unifying frame

Patient-safety research provides a useful lens because it already treats system failure, human error and organisational culture as central. Studies of hospital-acquired infection control show that safety depends on layered barriers, consistent protocols and a culture that reports failure [31]. These principles transfer almost directly to cybersecurity. A single technical defence is rarely sufficient, and resilient institutions assume that individual barriers will occasionally fail. This review adopts the patient-safety frame throughout.

3. Methods

3.1 Design and reporting standard

The review was designed and reported according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement, which updated the earlier 2009 guidance and clarified the reporting of search, selection and synthesis [32,33]. Because the field is heterogeneous in design and outcome, a scoping-style transparency approach was used to map the research landscape before synthesis. Methodological guidance on PRISMA-ScR, which stresses explicit mapping of concepts, evidence types and gaps, informed this stage [34,35]. Quantitative pooling (meta-analysis) was judged inappropriate because the included studies measured different outcomes with incompatible metrics. A narrative and thematic synthesis was therefore adopted. Other reviews of heterogeneous health evidence, such as work on trauma-related outcomes, show where meta-analysis becomes feasible, namely when outcomes and populations are sufficiently comparable [36].

3.2 Review questions

The questions were framed using a population–concept–context structure:

- **RQ1.** What cybersecurity vulnerabilities are most frequently reported in healthcare systems?
- **RQ2.** What data-privacy risks arise from the collection, sharing and secondary use of health data?
- **RQ3.** How do earlier reviews differ in method, scope and conclusions?
- **RQ4.** What technical, organisational, legal and equity-related responses are proposed, and what evidence supports them?

3.3 Eligibility, sources and search strategy

Table 1. Review protocol: eligibility criteria and search design

Domain	Specification
Population / setting	Hospitals, clinics, health information systems, telemedicine services, connected medical devices, public-health agencies
Concept	Cybersecurity threats, vulnerabilities, breaches, ransomware, privacy risk, data-protection regulation, mitigation
Study types included	Systematic reviews, narrative reviews, empirical studies, analyses of breach data, policy and legal analyses, authoritative technical guidance
Study types excluded	Opinion pieces without analytical content, studies unrelated to health data or health systems, duplicate publications
Period	2010 to 2025, plus foundational legal and technical sources
Language	English
Information sources	Biomedical, engineering and social-science bibliographic databases; regulatory texts; institutional reports; citation chaining from key reviews

Search concepts	(cybersecurity OR "information security" OR ransomware OR breach) AND (healthcare OR hospital OR "electronic health record" OR "medical device") AND (privacy OR confidentiality OR regulation)
Screening	Title and abstract, followed by full text; discrepancies resolved by consensus
Data items	Author, year, design, setting, threat or vulnerability type, outcome, mitigation proposed, limitations
Synthesis	Thematic analysis with cross-review comparison

3.4 Selection process

The PRISMA flow follows four standard stages. In the *identification* stage, records are retrieved from all sources and duplicates are removed. In *screening*, titles and abstracts are assessed against Table 1. In *eligibility*, full texts are examined and exclusions are recorded with reasons. In *inclusion*, the final corpus is assigned for extraction and synthesis. The numerical flow diagram should be completed from the search log, as set out in Section 4.1.

3.5 Appraisal and synthesis

Study quality was appraised qualitatively along four dimensions: transparency of method, appropriateness of data source, clarity of outcome definition and acknowledgement of limitations. Evidence was not excluded solely on quality grounds, because much of the relevant knowledge comes from breach registries, policy analyses and technical reports for which formal risk-of-bias tools are ill suited. Instead, the strength of each claim is reported alongside its source type. Codes were generated inductively and grouped into themes. Themes were then examined from four perspectives (technical, organisational, legal and equity) to test whether conclusions held across viewpoints.

3.6 Research integrity

The review followed established guidance on ethical conduct in research, which stresses honest reporting, accurate attribution and respect for source integrity [37]. All material is expressed in the authors' own analytical language and attributed through numbered citations. Work on plagiarism-free content creation, detection techniques and the use of AI in scholarly publishing underscores that originality rests on genuine synthesis and proper attribution, not merely on paraphrase [38–40].

4. Results

4.1 Study selection

The PRISMA 2020 flow records, in order:

- **Identification:** records identified from databases and registers ($n = [X]$); records from other methods, including citation chaining and regulatory repositories ($n = [Y]$); duplicates removed ($n = [Z]$).
- **Screening:** records screened by title and abstract ($n = [A]$); records excluded ($n = [B]$).
- **Eligibility:** reports assessed in full text ($n = [C]$); reports excluded with reasons ($n = [D]$).
- **Included:** studies and sources included in the synthesis ($n = [E]$).

The bracketed figures must be replaced with the counts from the actual search log before submission. The evidence discussed below is drawn from the corpus of reviews, empirical studies, regulatory instruments and policy analyses cited in this paper.

4.2 Characteristics of the evidence

The evidence base is heterogeneous in four ways. First, **design:** it comprises systematic and narrative reviews, retrospective impact analyses, breach-registry studies, technical security analyses, legal and sociological analyses, and framework documents. Second, **geography:** most empirical breach data come from the United States and the United Kingdom, with growing but thinner evidence from India, Australia and the Global South. Third, **outcome:** studies measure records exposed, financial cost, operational disruption, patient outcomes and regulatory compliance, which are not directly commensurable. Fourth, **time:** older studies address mostly paper-to-digital transitions, while recent ones deal with ransomware economies, cloud platforms and AI.

4.3 Thematic findings

Theme 1. A threat landscape dominated by ransomware, social engineering and human error

The most consistent finding across sources is the prominence of ransomware. A national analysis of attacks on delivery organisations documented a sustained and rising trend, with attacks spreading to clinics and smaller providers as well as large hospitals [11]. Ransomware affects availability first, and the clinical consequences follow. The WannaCry experience showed that a single unpatched vulnerability across many systems could simultaneously disable many institutions and divert emergency patients [9,10]. Disruption also propagates outward, because neighbouring emergency departments absorb the displaced patient volume and become strained themselves [12].

Human and organisational factors recur. A model of data-breach causation based on the "Swiss cheese" metaphor argues that breaches occur when weaknesses at several layers align, including individual behaviour, task design, supervision and organisational conditions [41]. A study of the US healthcare industry characterised many organisations as "muddling through" cybersecurity, responding reactively and under-investing relative to the risk [42]. Reviews of cybersecurity capability and hospital risk similarly emphasise gaps in staff awareness, patching discipline, asset inventories and incident planning [23–25]. Clinicians working under time pressure often choose workarounds that circumvent controls. Commentary on healthcare challenges in the era of cybersecurity stresses that the cultural distance between clinical and security priorities remains a persistent obstacle [43].

The comparative picture is consistent. Large, well-resourced institutions face more sophisticated attackers, while smaller providers face the same commodity attacks with fewer defences. In both cases, human-factor weakness is a recurring thread and not an exception.

Theme 2. Connected devices, smart environments and the expanding attack surface

Healthcare now contains thousands of networked endpoints beyond conventional computers: infusion pumps, imaging equipment, monitors, building systems and wearable sensors. An analysis of post-market surveillance data from medical devices found that a substantial number of reported problems involved software and security-related qualities, and that regulatory reporting systems were not designed to capture them well [44]. Devices often run legacy operating systems, cannot be patched without vendor involvement and remain in service for a decade or longer. These properties make them persistent weak points.

The same dynamic extends to the wider hospital environment. Work on machine learning for smart facility management shows how sensor data and automated control are entering hospital hospitality and building operations [45], which creates new links between operational technology and clinical networks. Sociological analyses of the smart home show how automation redistributes labour and introduces dependence on opaque systems [46], and analyses of smart cities highlight how urban technology can reproduce spatial and social divides [47]. These perspectives are not security studies, but they reinforce a security-relevant point: the more ambient and automated care environments become, the harder it is for users to understand, consent to or contest data flows.

AI introduces a further layer. Machine-learning systems for tasks such as predicting antimicrobial resistance patterns integrate genomic and epidemiological data [48]. Such systems depend on large, linked datasets, which concentrates sensitive information and creates attractive targets. The models themselves also become assets that can be manipulated or leaked. Diagnostic AI and AI-mediated patient engagement likewise depend on continuous data collection [2,3].

Theme 3. The limits of de-identification and the promise of privacy-enhancing technologies

A central privacy assumption has been that removing direct identifiers makes data safe to share. Empirical work challenges this belief. A study using generative statistical models estimated that a very high proportion of individuals in a large national population could be correctly re-identified from a small set of demographic attributes, even in incomplete datasets [49]. The implication is that "anonymised" data should often be treated as personal data, and that legal reliance on de-identification gives weaker protection than it appears to.

Technical responses have developed in parallel. Differential privacy offers a formal mathematical guarantee that the presence or absence of any single individual changes the output of an analysis only within a bounded amount,

which allows aggregate insight with controlled disclosure risk [50]. Federated learning allows models to be trained across institutions without centralising raw patient data, and has been proposed as a foundation for future digital health [51]. These approaches are promising but not complete. Federated systems can still leak information through model updates, differential privacy involves a trade-off between accuracy and protection, and both require specialist capability that many providers lack.

Privacy risk is also generated by algorithmic design. Analysis of algorithmic bias shows that AI systems can reproduce and amplify social stratification, with unequal error rates and unequal visibility across groups [52]. In a health context, biased models trained on non-representative records can generate privacy-relevant harms, such as disproportionate surveillance, inaccurate risk labelling or exclusion from services.

Theme 4. Organisational culture, leadership and workforce

Security outcomes are strongly shaped by leadership. Studies of effective hospital leadership describe how leadership style influences accountability, communication and willingness to invest in preventive measures [14]. Crisis leadership scholarship argues that institutions improve when they treat failures as occasions for learning and not blame [15]. Work on embedding trauma-informed principles into healthcare leadership describes a paradigm shift in organisational culture and patient outcomes [53], and its emphasis on psychological safety is directly relevant: staff who fear punishment are less likely to report phishing clicks or near-misses, and under-reporting blinds the organisation.

The physical and educational environment of care also matters. Evidence-based environmental design and educational interventions are associated with better health outcomes [54], and similar logic applies to digital environments, where well-designed interfaces and training reduce error. Experience from infection control demonstrates that sustained behavioural change requires protocols, monitoring and feedback and not one-off instruction [31]. Cybersecurity awareness programmes that consist of an annual slide deck are unlikely to meet this standard.

Theme 5. Inequity, stigma and the unequal distribution of privacy harm

Privacy harms do not fall evenly. Where health disparities are structural, breaches and misuse affect already disadvantaged groups most severely. A socio-legal study of health disparities in Punjab documents structural inequities and legislative gaps that limit access to equitable care [55]. Broader analyses of disease burden and epidemiological transition in India show a population facing both communicable and non-communicable disease at scale, and therefore a large volume of sensitive health data collected from people with limited ability to negotiate its use [56,57]. Research on cancer-related stigma shows that disclosure of a diagnosis can lead to social exclusion and psychological harm [58], so a breach of oncology or mental-health records carries consequences that extend beyond the clinical setting.

The same logic applies to digital access. Telemedicine can widen access, yet its benefits and risks vary across socioeconomic groups [4]. Patients with lower digital literacy may be less able to recognise phishing, understand consent screens or exercise rights over their data. Equity should therefore be treated as a security requirement and not as an afterthought.

Theme 6. Fragmented and uneven legal frameworks

Legal analysis shows that health legislation is a structural component of national health systems, shaping institutional duties and accountability [59]. Sociological perspectives on law emphasise that legal rules only constrain behaviour when social and institutional conditions support enforcement [60]. Concepts from tort law are relevant as well. Negligence doctrine asks whether a duty of care existed, whether it was breached and whether harm resulted [61], and as ransomware outcomes become foreseeable, the argument that failing to implement reasonable safeguards constitutes a breach of duty strengthens. Scholarship on law and ethical business practice argues that legislation can be an instrument for promoting responsible corporate conduct [62], a perspective applicable to technology vendors and cloud providers serving the health sector.

Comparison of regimes (Table 3) shows convergence on principles such as lawful processing, security safeguards and breach notification, but divergence in scope, enforcement intensity and the treatment of cross-border transfer. Rule-based, sector-specific approaches such as HIPAA differ from comprehensive rights-based regimes such as

the GDPR, while consent-centred statutes such as India's 2023 Act place considerable weight on notice and consent mechanisms, which may be difficult for vulnerable users to exercise meaningfully.

Theme 7. Systemic resilience: infrastructure, supply chains and work arrangements

Cyber resilience depends on the wider system. Analysis of flood impacts on health systems shows how physical hazards can disable healthcare infrastructure, strain economic capacity and expose vulnerability in service delivery [63]. Cyber-attacks and physical disasters share a logic, since both degrade availability and test continuity planning. Compound events, such as an attack during a disaster, are plausible and poorly studied.

Geopolitical supply-chain competition affects the sourcing and trust of hardware, software and cloud services [64], which matters for institutions that depend on foreign-built components. Changes in work arrangements add further risk. Research on remote work and the weakening of informal social capital suggests that dispersed staff may have fewer informal cues for spotting suspicious activity [65], and remote access expands the perimeter that must be defended. Post-pandemic changes in relationships and household dynamics also increase the use of home networks and personal devices for health-related activity [66].

5. Comparative Analysis of Related Research Reviews

A credible systematic review must be positioned against earlier syntheses. Table 2 compares the principal reviews, their scope, their characteristic findings and the gaps that remain.

Table 2. Comparison of related reviews on healthcare cybersecurity and privacy

Review (ref.)	Scope and approach	Principal findings or outputs	Remaining gap
Fernández-Alemán et al. [18]	Systematic literature review of security and privacy in electronic health records	Catalogued security requirements, controls and privacy concerns around access control, authentication and data sharing	Predates ransomware era, cloud and AI; little organisational analysis
Kruse et al. [6]	Systematic review of threats and trends	Identified malware, phishing, insider threats and unencrypted data as dominant concerns; noted scarcity of evidence on mitigation	Limited evaluation of intervention effectiveness
Coventry and Branley [19]	Narrative review of trends, threats and ways forward	Highlighted human behaviour, legacy systems and the need for cultural change alongside technology	Narrative design limits reproducibility
Jalali and Kaiser [20]	Systematic, organisational perspective	Framed hospital security as socio-technical and organisational, emphasising governance and process	Less emphasis on privacy law and equity
Argaw et al. [21]	Discussion of hospital cybersecurity challenges and mitigation	Outlined risks from connected devices, resource constraints and fragmented responsibility	Limited comparative regulatory analysis
Seh et al. [22]	Analysis of breach data and implications	Showed recurring breaches and large-scale exposure of records; derived implications for protection	Descriptive; little on causal mechanisms
Sardi et al. [23]	Systematic review of cyber risk in health facilities	Mapped risk assessment and management approaches, noting heterogeneity of methods	Few outcome-based validations
Wasserman and Wasserman [24]	Review of hospital risks and gaps for non-specialists	Translated technical risk into accessible gaps for clinicians and managers	Not primarily systematic
Offner et al. [25]	Systematic review of capability in Australian healthcare	Examined trends, threats and mitigation, with attention to national capability	Single-country focus
Ahluwalia [1]	Systematic review of digital transformation	Linked digitisation to management, efficiency and organisational change	Security treated as one dimension among many

	in management	hospital	
--	------------------	----------	--

5.1 Points of convergence

Across these reviews, four conclusions recur. First, human behaviour and organisational culture are as important as technology [6,19,20]. Second, legacy and connected systems create persistent vulnerability [21,23]. Third, breaches are frequent and large, and available data probably understate the true figure because of under-reporting [7,22]. Fourth, evidence on the effectiveness of specific mitigations is weaker than evidence on threats [6,23]. The last point is the most consequential for practice: organisations are being asked to invest in controls whose benefit is documented mainly by analogy and expert opinion.

5.2 Points of divergence

The reviews diverge in three respects. Earlier work centred on records and access control [18], whereas later work shifted toward ransomware, availability and operational disruption [11,12]. Some reviews adopt an organisational lens [20] while others emphasise technical catalogues of threats [6,21], which produces different policy implications: governance reform in the first case, tool acquisition in the second. Finally, reviews differ in geographic frame, with most evidence drawn from high-income settings [7,25], leaving the experience of low- and middle-income systems underdeveloped.

5.3 Comparative quantitative indicators

Table 2 is complemented by reported quantitative indicators from the primary and secondary sources, which illustrate scale and trend without implying that the figures are directly comparable.

Table 3. Selected comparative indicators reported in the literature

Indicator	Source (ref.)	Reported finding (as stated by source)	Interpretation
Reportable breaches, United States, 2010–2017	[7]	More than two thousand breaches, affecting well over one hundred million records	Breaches are routine and large-scale
Average cost of a data breach in healthcare	[8]	Above US\$10 million in recent editions, the highest of the sectors surveyed	Healthcare is the costliest sector for breaches
Ransomware attacks on delivery organisations, 2016–2021	[11]	Several hundred attacks, with annual numbers rising over the period	Attack frequency is increasing
Re-identification risk from demographic attributes	[49]	A very high share of individuals re-identifiable from about fifteen attributes	De-identification alone is insufficient
NHS WannaCry disruption, 2017	[9]	Thousands of cancelled appointments and many affected organisations	Availability attacks harm patients directly

The exact figures should be verified against the cited publications before submission, since the reported values depend on dataset, period and definition.

6. Comparative Analysis of Regulatory Frameworks

Table 4. Comparison of three data-protection frameworks relevant to health data

Feature	GDPR (EU) [27]	HIPAA (USA) [28]	DPDP Act 2023 (India) [29]
Legal nature	Comprehensive, rights-based regulation across all sectors	Sector-specific federal statute and rules	Comprehensive, consent-based statute

Health data	Special category with heightened conditions for processing	Protected health information held by covered entities and business associates	Personal data generally; no separate sensitive category in the statute
Core obligations	Lawful basis, purpose limitation, minimisation, security, accountability	Privacy Rule, Security Rule, minimum necessary standard	Notice, consent, purpose limitation, security safeguards by data fiduciaries
Breach notification	Notification to authority and, where high risk, to individuals, within a short statutory window	Notification to individuals, regulator and, for large breaches, the media	Notification to the Data Protection Board and affected persons
Individual rights	Access, rectification, erasure, portability, objection	Access and amendment; accounting of disclosures	Access, correction, erasure, grievance redressal
Enforcement	Independent authorities; substantial administrative fines	Federal regulator; civil and criminal penalties	Data Protection Board; monetary penalties
Principal critique	Compliance complexity, uneven enforcement	Does not reach many non-covered health apps and data brokers	Heavy reliance on consent; exemptions for the state

The comparison supports three analytical observations. First, **scope** determines protection. A sector-specific statute leaves gaps when health data move outside covered entities, for example into consumer applications. A comprehensive regime closes some of these gaps but at the cost of complexity. Second, **consent** is an imperfect safeguard. Where individuals have limited literacy, choice or alternatives, consent can become a ritual, which is particularly problematic in settings with large socioeconomic disparities [4,55]. Third, **enforcement capacity** matters as much as statutory text, consistent with sociological views that the effect of law depends on institutional support [60].

7. Discussion: Analysis from Different Perspectives

7.1 The technical perspective

Technically, the evidence supports defence in depth: asset inventory, network segmentation, timely patching, strong authentication, encryption, logging, tested backups and rehearsed recovery. Segmentation limits lateral movement, which is crucial given the evidence of simultaneous multi-institution disruption [9]. Immutable, offline backups reduce the leverage of ransomware, since the attacker's threat depends on irreversibility. For devices that cannot be patched, compensating controls such as isolation, monitoring and vendor accountability are required [44].

Privacy-enhancing technologies should be adopted selectively. Where re-identification risk is high [49], organisations should presume that de-identified data remain personal, restrict access through controlled environments and consider differential privacy [50] or federated approaches [51]. These are not substitutes for governance but complements to it.

A less-discussed technical issue is AI itself. Diagnostic and engagement systems [2,3] and predictive models [48] concentrate data and depend on model integrity. Security assessment should extend to training data provenance, model access and output monitoring, and fairness assessment should accompany security assessment because biased systems create their own privacy harm [52].

7.2 The organisational and leadership perspective

Organisational evidence suggests that the principal bottleneck is often governance and not technology. Leadership style shapes risk tolerance and resource allocation [14]. Institutions that learn from crises and share lessons transparently improve more quickly [15]. Psychological safety, a theme in trauma-informed leadership [53], is a security asset: it increases reporting of suspicious messages and near-misses and reduces concealment.

Burnout and administrative burden, which affect healthcare professionals, interact with security. Exhausted staff are more likely to bypass controls or fall for deceptive messages. The patient-safety tradition argues that systems

must be designed for fallible people and not for ideal ones [31], and the same expectation should apply to authentication workflows, access requests and incident reporting. Environmental and educational design [54] suggests that interventions work best when they are embedded in daily practice and not delivered as occasional lectures.

7.3 The legal and ethical perspective

The legal analysis reveals a paradox. Regulations proliferate, yet the health data ecosystem is still full of gaps. Legislation can strengthen national health systems [59], but only when it is clear, enforceable and aligned with operational reality. Tort principles suggest an additional accountability channel. As the risks of ransomware and basic hygiene failures become well documented, claims that an organisation took reasonable care become harder to sustain [61]. Law can also be used to promote ethical conduct in business more broadly [62], which supports contractual and statutory duties for vendors, cloud providers and processors.

Ethical analysis adds a further dimension. Research ethics stresses respect, honesty and the protection of participants [37], and the same values should govern secondary use of health data. Patients rarely anticipate that their records may be used to train commercial algorithms, and meaningful transparency requires more than a long consent notice.

7.4 The equity and social perspective

Equity is the least developed theme in the cybersecurity literature and one of the most important. Digital health is not equally accessible [4], and structural health disparities shape who is exposed to risk [55–57]. Stigmatised conditions raise the cost of disclosure [58]. Algorithmic systems may exacerbate stratification [52], and automated environments, from the home to the city, redistribute burdens in unequal ways [46,47]. A security programme that protects average patients but ignores those with low literacy, limited connectivity or high stigma exposure will leave the greatest harms unaddressed.

7.5 The geopolitical and systemic perspective

Health data are increasingly entangled with state interests. Digital surveillance practices raise concerns about sovereignty and rights, particularly in the Global South [16], and the use of the internet as an instrument of statecraft means that health institutions can become collateral or deliberate targets [17]. Supply-chain competition raises questions about hardware and software provenance [64]. Resilience planning must therefore consider geopolitical dependencies alongside conventional technical risk, and must be integrated with disaster preparedness, since physical and cyber events can compound each other [63].

7.6 Synthesis: an integrated framework

The perspectives above point to a layered model, summarised below.

- **Govern.** Establish board-level accountability, a named responsible executive, risk appetite statements and learning-oriented incident review [14,15].
- **Know.** Maintain a live inventory of assets, data flows and third-party dependencies, including connected devices and AI systems [44,48].
- **Protect.** Apply segmentation, patching, multi-factor authentication, encryption and tested offline backups [9,11].
- **Minimise and anonymise honestly.** Collect only what is needed, treat de-identified data with caution and use privacy-enhancing technologies where suitable [49–51].
- **Prepare people.** Provide continuous, role-specific training within a psychologically safe culture [31,53].
- **Include.** Design consent, notice and support for diverse literacy, language and stigma-risk profiles [4,55,58].
- **Comply and be accountable.** Map obligations across jurisdictions and treat foreseeable cyber risk as part of the duty of care [27–29,61].
- **Recover.** Rehearse downtime procedures, maintain clinical continuity plans and integrate cyber events with disaster planning [12,63].

7.7 Implications for research

The evidence base shows five priorities. First, intervention research is needed to establish which controls reduce harm, since the existing literature documents threats more thoroughly than remedies [6,23]. Second, outcome studies should link attacks to patient-level clinical outcomes, extending early work on care quality [13]. Third, research from low- and middle-income settings is scarce relative to need. Fourth, the equity and stigma dimensions of privacy require systematic study [55,58]. Fifth, methodological transparency in reviews should improve, with wider use of PRISMA-based reporting and scoping approaches to map heterogeneous evidence [32,34,35].

8. Recommendations

For healthcare organisations. Treat cybersecurity as a clinical-risk domain governed at board level [14]. Fund resilience and recovery capability and not only prevention. Run regular downtime exercises that include clinical staff. Adopt a no-blame reporting culture [15,53].

For clinicians and managers. Participate in the design of security workflows so that controls fit real practice. Escalate unsafe workarounds as patient-safety issues, in line with established safety culture [31].

For policymakers and regulators. Close scope gaps between sector-specific and general regimes. Strengthen enforcement capacity and mandate timely, transparent breach reporting [27–29]. Support smaller providers through shared services and subsidised security baselines. Consider requiring security-by-design obligations for device manufacturers and software vendors [44].

For technology developers. Design for patchability, minimal data collection and auditability. Test AI systems for bias and for privacy leakage before deployment [52]. Document data provenance.

For researchers. Conduct and register protocols for intervention studies. Report outcomes in patient-centred terms. Use consistent definitions of breach, incident and impact to allow meaningful comparison [32].

9. Limitations

This review has several limitations. First, the evidence is heterogeneous in design, outcome and setting, which prevented quantitative pooling and required narrative synthesis. Second, breach data are subject to under-reporting and to definitional variation across jurisdictions, so reported figures probably understate real incidence [7,22]. Third, the literature is concentrated in high-income countries, which limits generalisability to settings with different infrastructure and legal systems. Fourth, the field moves quickly. Ransomware tactics, regulatory instruments and AI deployment change faster than the publication cycle, so some findings may be outdated by the time of reading. Fifth, a number of included sources are analytical, policy-oriented or sociological and are not formal empirical studies, and formal risk-of-bias tools could not be applied uniformly. Finally, the English-language restriction may have excluded relevant regional evidence.

10. CONCLUSION

Modern healthcare systems are exposed to cybersecurity and privacy risks that are frequent, costly and clinically consequential. The evidence reviewed here shows that the main threats are ransomware, social engineering, insider error and insecure connected devices, and that de-identification offers weaker protection than commonly assumed. Organisational culture and leadership determine whether technical controls are implemented and sustained. Legal frameworks converge in principle but diverge in scope and enforcement, leaving gaps that disadvantaged and stigmatised populations are least able to absorb.

Four conclusions follow. First, cybersecurity in healthcare is a patient-safety discipline and should be governed as one. Second, technology without governance, training and psychological safety will fail. Third, privacy protection must be designed for equity, since harms are unevenly distributed. Fourth, the research base needs more intervention studies, more patient-level outcome data and greater attention to low- and middle-income settings. A layered and equity-aware model of security by design, supported by clear law and learning-oriented leadership, offers the most credible route to protecting both patient data and the care that depends on it.

REFERENCES

1. Ahluwalia PS. Assessing the impact of digital transformation on hospital management: a systematic review. *Int J Healthc Hosp Manag Stud*. 2025;1–16.
2. Ahluwalia PS. Artificial intelligence in healthcare: the role of artificial intelligence in diagnostic medicine. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;164–75.
3. Ahluwalia PS. Redesigning patient engagement in AI-driven healthcare systems: an analysis. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;203–17.
4. Ahluwalia PS. Digital health equity: evaluating access and outcomes in telemedicine across socioeconomic groups. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;84–92.
5. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? *BMJ*. 2017;358:j3179.
6. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care*. 2017;25(1):1–10.
7. McCoy TH, Perlis RH. Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA*. 2018;320(12):1282–4.
8. IBM Security. Cost of a data breach report 2023. Armonk (NY): IBM Corporation; 2023.
9. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digit Med*. 2019;2:98.
10. Gordon WJ, Fairhall A, Landman A. Threats to information security — public health implications. *N Engl J Med*. 2017;377(8):707–9.
11. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum*. 2022;3(12):e224873.
12. Dameff C, Tully J, Chan TC, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Netw Open*. 2023;6(5):e2312270.
13. Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res*. 2019;54(5):971–80.
14. Ahluwalia PS. Healthcare leadership and management: effective leadership styles in hospital administration. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;69–82.
15. Ahluwalia PS. Crisis leadership in healthcare: organizational learning from pandemic failures. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;136–46.
16. Ahluwalia PS. The rise of techno-authoritarianism: digital surveillance and sovereignty in the Global South. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;34–54.
17. Ahluwalia PS. Cyber-diplomacy and conflict: how states weaponize the internet in 21st century geopolitics. *Siddhanta's Int J Adv Res Arts Humanit*. 2025;157–71.
18. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform*. 2013;46(3):541–62.
19. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas*. 2018;113:48–52.
20. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *J Med Internet Res*. 2018;20(5):e10059.
21. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, et al. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak*. 2020;20(1):146.
22. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare data breaches: insights and implications. *Healthcare (Basel)*. 2020;8(2):133.
23. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber risk in health facilities: a systematic literature review. *Sustainability*. 2020;12(17):7002.
24. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: review (for the non-cyber professional). *Front Digit Health*. 2022;4:862221.
25. Offner KL, Sitnikova E, Joiner K, MacIntyre CR. Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intell Natl Secur*. 2020;35(4):556–85.
26. National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity, version 1.1. Gaithersburg (MD): NIST; 2018.
27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Off J Eur Union*. 2016;L119:1–88.
28. Health Insurance Portability and Accountability Act of 1996, Pub L No. 104-191, 110 Stat 1936 (1996).

29. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Government of India; 2023.
30. World Health Organization. Global strategy on digital health 2020–2025. Geneva: World Health Organization; 2021.
31. Ahluwalia PS. Improving patient safety: strategies for reducing hospital-acquired infections. *Siddhanta's Int J Adv Res Arts Humanit.* 2024;126–45.
32. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ.* 2021;372:n71.
33. Moher D, Liberati A, Tetzlaff J, Altman DG; PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS Med.* 2009;6(7):e1000097.
34. Ahluwalia PS. Enhancing systematic transparency through PRISMA-ScR: a scoping review approach for emerging researchers. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;1–27.
35. Ahluwalia PS. Structured exploration through PRISMA-ScR: a transparent method for mapping research landscapes. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;137–67.
36. Elliason EK, Ahluwalia PS. Prevalence and predictors of trauma-related mental health outcomes among refugees and internally displaced persons in Africa during conflict and crisis: a systematic review and meta-analysis. *Interdiscip J Afr Alliance Res Advocacy Innov.* 2025;1(2).
37. Ahluwalia PS. Ethical issues in social science research. *Shodh Patra Int J Multidiscip Stud.* 2024;1–8.
38. Ahluwalia PS. How we make plagiarism-free content: theory and practices. *Shodh Prakashan J Humanit Soc Sci.* 2025;46–53.
39. Ahluwalia PS. Plagiarism: detection techniques and tools. *Siddhanta's Int J Adv Res Arts Humanit.* 2024;1–11.
40. Ahluwalia PS. The role of artificial intelligence in combating plagiarism in scholarly publishing. *Shodh Prakashan J Humanit Soc Sci.* 2025;26–30.
41. Kamoun F, Nicho M. Human and organizational factors of healthcare data breaches: the Swiss cheese model of data breach causation and prevention. *Int J Healthc Inf Syst Inform.* 2014;9(1):42–60.
42. Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: insights from the U.S. healthcare industry. *Bus Horiz.* 2019;62(4):539–48.
43. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. *Health Secur.* 2020;18(3):228–31.
44. Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, Fu K, et al. Security and privacy qualities of medical devices: an analysis of FDA postmarket surveillance. *PLoS One.* 2012;7(7):e40200.
45. Singh P. Integrating machine learning for smart facility management in healthcare hospitality environments. *Shodh Patra Int J Multidiscip Stud.* 2025;82–92.
46. Ahluwalia PS. Invisible labor in the smart home: a sociological look at gender, automation, and domesticity. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;143–56.
47. Ahluwalia PS. Smart cities and social divide: spatial justice in the age of urban tech. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;185–202.
48. Ahluwalia PS. Artificial intelligence-driven prediction of antimicrobial resistance patterns: integrating machine learning with genomic epidemiology for precision antibiotic stewardship. *J Integr Res.* 2025;97–122.
49. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun.* 2019;10:3069.
50. Dwork C, Roth A. The algorithmic foundations of differential privacy. *Found Trends Theor Comput Sci.* 2014;9(3–4):211–407.
51. Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, et al. The future of digital health with federated learning. *NPJ Digit Med.* 2020;3:119.
52. Ahluwalia PS. Algorithmic bias and social stratification: how AI shapes inequality in digital societies. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;28–37.
53. Ahluwalia PS, John S, Elliason EK. Embedding trauma-informed care into healthcare leadership: a paradigm shift in organizational culture and patient outcomes. *Interdiscip J Afr Alliance Res Advocacy Innov.* 2025;1(2).
54. Ahluwalia PS. Transforming healthcare outcomes through evidence-based environmental design and educational interventions. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;279–318.
55. Singh D, Ahluwalia PS. A socio-legal study on health disparities in Punjab: structural inequities, legislative gaps, and pathways to equitable healthcare. *Shodh Prakashan.* 2026;1–14.
56. Ahluwalia PS. Disease burden in India: a comprehensive analysis. *Siddhanta's Int J Adv Res Arts Humanit.* 2025;179–235.
57. Ahluwalia PS, John S. Disease pattern/trends in India: a comprehensive analysis of epidemiological transitions and public health challenges (2020–2025). *Siddhanta's Int J Adv Res Arts Humanit.* 2025;20–51.

58. Elliason EK, Singh K, Singh AP. Breaking the silence: understanding cancer-related stigma among tertiary students in Punjab. *Siddhanta's Int J Adv Res Arts Humanit.* 2025:1–24.
59. Ahluwalia PS, John S. The role of health legislation in strengthening national health systems: a policy-legal perspective. *Interdiscip J Anal Educ Sci Commer Manag Law.* 2025:1–20.
60. Ahluwalia PS, Singh D. The sociology of law: understanding the relationship between law, society, and social control. *Siddhanta's Int J Adv Res Arts Humanit.* 2026:142–8.
61. Ahluwalia PS. Negligence under law of torts. *Shodh Prakashan.* 2025:1–18.
62. Ahluwalia PS. Corporate social responsibility and the law: the role of legislation in promoting ethical business practices. *Shodh Prakashan J Law Judicial Syst.* 2025;1(1):42–51.
63. Ahluwalia PS. Impacts of floods on health and healthcare systems in Asian countries: a comprehensive analysis of direct and indirect health consequences, economic burden, and healthcare infrastructure vulnerability. *Shodh Prakashan.* 2025:72–102.
64. Ahluwalia PS. Decoupling and the new Cold War: US-China strategic competition in the global supply chain. *Siddhanta's Int J Adv Res Arts Humanit.* 2025:55–70.
65. Ahluwalia PS, Kumar A. Remote work and the death of the watercooler: changing social capital in the post-office era. *Siddhanta's Int J Adv Res Arts Humanit.* 2025:110–22.
66. Ahluwalia PS, Elliason EK. Post-pandemic intimacy: reconfiguring relationships and family dynamics in a hybrid world. *Siddhanta's Int J Adv Res Arts Humanit.* 2025:69–77.