Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 05| Issue- 04| 2026

Research Article **Received:** 05-03-2026 | **Accepted:** 31-03-2026 | **Published:** 17-04-2026

Designing Compliance-Driven Cybersecurity Governance Models for Hipaa-Regulated Healthcare Systems

Nicholas Addotey

Montana State University

Abstract: Healthcare organizations continue to experience escalating ransomware attacks, third-party breaches, and operational disruptions despite widespread compliance with the Health Insurance Portability and Accountability Act (HIPAA). This pattern suggests that regulatory adherence alone does not ensure effective cybersecurity risk reduction. This study argues that the persistent gap between formal HIPAA compliance and real-world security outcomes is fundamentally a governance failure rather than a regulatory deficiency. Drawing on breach trend data from the HHS Office for Civil Rights, the Verizon Data Breach Investigations Report, and ransomware impact studies published in JAMA Health Forum, this paper demonstrates that weak executive oversight, diffuse risk ownership, inadequate third-party governance, and slow escalation processes contribute materially to breach severity and operational disruption. In response, the paper proposes a compliance-driven cybersecurity governance model that operationalizes HIPAA safeguards through structured accountability, defined decision authority, continuous oversight, and measurable governance performance indicators. The model integrates board-level risk oversight, executive risk ownership, compliance–security alignment, and operational enforcement into a unified governance system designed for vendor-dependent, clinically sensitive healthcare environments. An evaluation framework is introduced to assess governance effectiveness using behavioral metrics such as risk ownership completeness, escalation timeliness, vendor monitoring coverage, and incident containment performance rather than audit artifact completion. By reframing HIPAA compliance as an enforceable governance system rather than a documentation exercise, this study contributes a structured model for strengthening healthcare cybersecurity resilience and establishes a foundation for future empirical validation of governance-driven risk reduction.

Keywords: Healthcare cybersecurity, Ransomware risk, Data breaches, Information security governance, Regulatory enforcement.

INTRODUCTION

Healthcare has become one of the most targeted sectors for cyberattacks. Hospitals, clinics, insurers, and health information exchanges store large volumes of sensitive patient data, including medical histories, insurance information, and personal identifiers (Kruse *et al*., 2017). This data is highly valuable in criminal markets and is often housed within complex systems that combine legacy systems with modern digital platforms. As a result, healthcare organizations experience ransomware attacks, data theft, service disruptions, and privacy violations at rates higher than many other critical sectors. These incidents lead not only to financial losses but also threaten patient safety, disrupt clinical operations, and erode public trust (Jalali & Kaiser, 2018.

In response, healthcare organizations in the United States rely heavily on compliance with the Health Insurance Portability and Accountability Act (HIPAA) as the primary benchmark for cybersecurity readiness. McLeod & Dolezel, 2018). HIPAA establishes administrative, physical, and technical safeguards to protect electronic protected health information (ePHI) (McLeod & Dolezel, 2018). However, repeated large-scale breaches demonstrate that regulatory compliance alone does not guarantee effective security. Several breached organizations were technically HIPAA-compliant at the time of the incident, indicating a persistent gap between formal adherence and actual risk reduction (Gordon *et al*., 2021).

Traditional cybersecurity approaches in healthcare have emphasized technical controls such as firewalls, access controls, and encryption. While these measures are necessary, they are insufficient in isolation. Cybersecurity failures are frequently rooted in governance weaknesses rather than technology flaws (Zhang *et al*., 2021). Such weaknesses include unclear accountability for security decisions, limited executive oversight, underfunded security programs, and poor coordination among compliance, risk management, and IT operations. When governance structures are weak, security controls are applied inconsistently, risks are not escalated appropriately, and compliance–devolves into a procedural exercise rather than a proactive mechanism.

This reality has led to a growing shift from purely technical security models toward governance-centered approaches. Cybersecurity governance focuses on how security decisions are made, how risk ownership is assigned, how priorities are

***Corresponding Author:** Nicholas Addotey

DOI- https://doi.org/10.5281/zenodo.19635109

determined, and how compliance requirements are enforced across the enterprise. Effective governance emphasizes leadership engagement, defining roles, risk accountability, and continuous oversight. While established frameworks from the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) recognize governance as foundational to cybersecurity, these frameworks are often applied generically and are not consistently adapted to the regulatory and operational realities of HIPAA-regulated healthcare systems (Hoffmann *et al*., 2020).

The motivation for the research stems from the lack of governance models that explicitly integrate HIPAA compliance with cybersecurity risk management and executive decision-making. Existing studies tend to examine compliance, security controls, or governance structures in isolation (Alshaikh *et al*., 2021). Few studies offer a structured model that explains how governance mechanisms can actively enforce HIPAA safeguards and reduce breach risk in practice. This paper argues that governance constitutes the missing layer connecting policy requirements to day-to-day security operations. By reframing HIPAA compliance as a governance challenge rather than a technical checklist, healthcare organizations can move toward more resilient and accountable cybersecurity programs. Ultimately, this study seeks to shift the focus from whether organizations are compliant to whether they are genuinely secure (Zhang *et al*., 2021).

OVERVIEW OF HIPAA SECURITY AND PRIVACY REQUIREMENTS

HIPAA requires covered entities and business associates to protect electronic protected health information through administrative, physical, and technical safeguards. In practice, however, the primary weakness lies not in the structure of these safeguards but in their implementation. Many organizations treat HIPAA requirements as a compliance task rather than as mechanisms for continuous risk control. This creates a persistent gap between written policy and operational enforcement (Viswanathan *et al*., 2025). Empirical research indicates that cyber intrusions and IT incidents are now the most common breach categories in healthcare, and both the frequency and scale of breaches have increased over time (Bonsu & Opoku, 2025). HIPAA's implementation flexibility allows organizations to meet minimum regulatory requirements while remaining vulnerable to modern attack methods such as credential theft, ransomware, and exploitation of unpatched systems (Seh *et al*., 2020). As a result, formal compliance does not necessarily translate into effective risk reduction.

Healthcare Cybersecurity Governance

Cybersecurity governance defines how security decisions are made, how risk ownership is assigned, how leadership gains visibility into exposure, and how enforcement is sustained. In healthcare environments, governance failure, such as unclear accountability and delayed decision-making, often contributes more significantly to security breakdowns than purely technical deficiencies. (Agarwal & Shah, 2024). Findings from the Verizon Data Breach Investigations Report (DBIR) Healthcare Snapshot highlight the governance dimension of many breaches. The "human element" was present in 68% of breaches, errors contributed to 28%, and third-party involvement accounted for 15% (a 68% increase from the prior year's definition and measurement approach) (Gellert *et al*., 2025). These numbers point to governance problems: training quality, workflow design, approval paths, vendor selection, and oversight, not just "missing technology."

The DBIR further indicates that extortion has become a dominant breach driver. Approximately one-third (32%) of breaches involved ransomware or related extortion techniques, with traditional ransomware accounting for 23% (Singh, 2025). Extortion incidents rapidly escalate into operational crises, requiring immediate coordination and recovery prioritization. When governance structures lack clarity, responses can amplify damage. Peer-reviewed evidence reinforces the patient safety implications of such disruptions. A study published by JAMA Network Open found that ransomware attacks on US healthcare delivery organizations increased over time and were associated with electronic system downtime and care disruption, elevating cybersecurity risk beyond data loss to patient safety concerns (Neprash *et al*., 2022; Alla *et al*., 2025).

HIPAA Compliance and Audit Limitations

A consistent finding in the literature is that compliance–assessments frequently focus on the existence of policies and documented controls rather than their effectiveness under operational stress.

Publisher: SARC Publisher

Two data points illustrate this limitation. First, incident patterns from the Verizon Data Breach Investigations Report indicate that the median time for users to engage with phishing emails is under 60 seconds (Verizon. (2024). This proves that training alone is insufficient. Effective governance must require layered protections such as Multi-factor Authentication (MFA), phishing-resistant authentication mechanisms, and clearly define escalation pathways because user error can occur rapidly (Jalali *et al*., 2020; Zhang *et al*., 2024). Second, breach cost and containment data underscore the inadequacy of minimal compliance. The IBM Security Cost of a Data Breach Report 2024 identifies healthcare as the costliest industry for breaches, with an average cost of USD 9.77 million. The mean time to identify and contain a breach was–258 days (IBM Security & Ponemon Institute 2024; Ahmed *et al*., 2025). These figures highlight the need for continuous monitoring and a defined containment authority rather than checklist driven assessments.

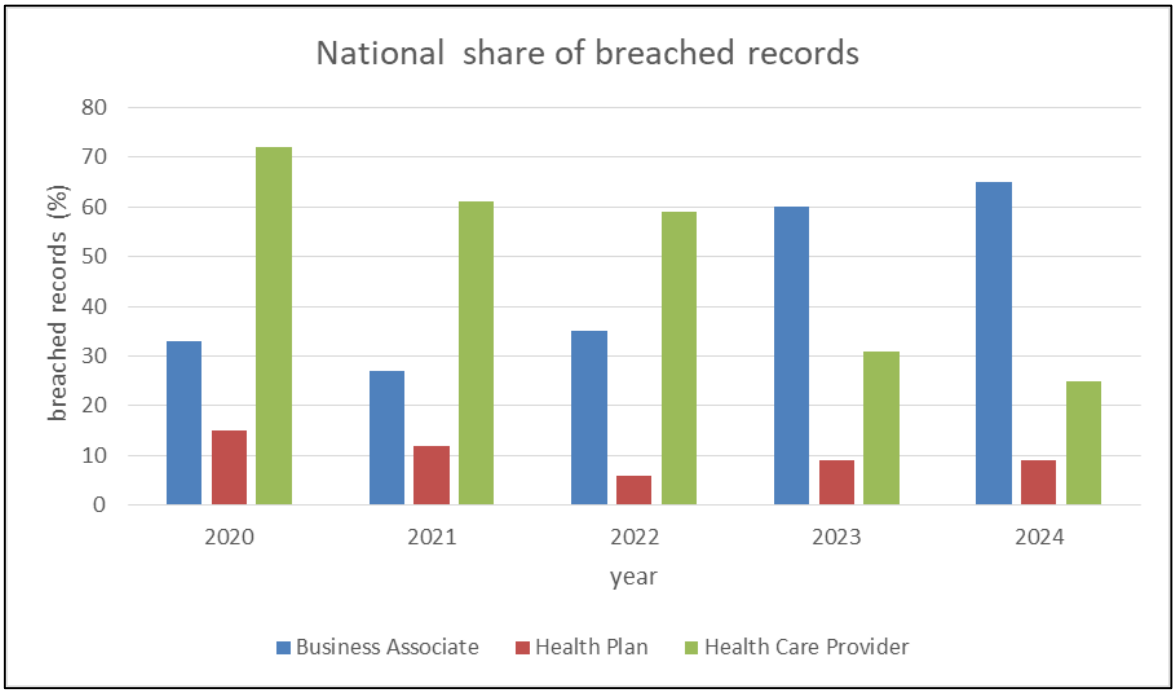

Figure 1: Distribution of Breached Healthcare Records by Entity Type (2020–2024).

The share of breached records linked to business associates rose sharply from 33% in 2020 to 65% in 2024, while the provider share fell from 72% to 25%, and the health plan share remained low (6–15%). This suggests breach impact is shifting toward third-party vendors and highlights the need for stronger vendor governance, not just internal HIPAA compliance (Ahmed *et al*., 2025; Subramanian *et al*., 2024; Neprash *et al*., 2022).

CONCEPTUAL FRAMEWORK FOR COMPLIANCE-DRIVEN CYBERSECURITY GOVERNANCE

Healthcare organizations continue to face cybersecurity failures due to unclear decision-making authority, weak oversight, and inconsistent follow-through. Broader evidence indicates that most breaches stem from hacking and IT-related incidents, and that the overall frequency of these attacks continues to grow (Seh *et al*., 2020). These patterns make it clear that the issue is not simply about failing technologies; it reflects deeper weaknesses in how healthcare organizations govern cybersecurity risk. The framework reconceptualizes HIPAA not as paperwork, but as an enforcement system that shapes responsibility assignment, resource allocation, vendor management, and response to incidents. It is designed for HIPAA-regulated systems where clinical uptime, third-party dependence, and privacy obligations collide.

Compliance-driven cybersecurity governance

Compliance-driven cybersecurity governance is a structured way of directing and controlling cybersecurity in which HIPAA obligations are translated into decision authority, accountability, and continuous oversight. In simple terms, it operationalized four enforceable questions: ***who owns each category of HIPAA-related risk***, ***who determines remediation priority***, ***how control effectiveness is validated in daily operation (how the organization knows safeguards are working***

Publisher: SARC Publisher

day to day and not only during audits), and ***what happens when a required safeguard is weak, ignored, or delayed***. Many organizations treat HIPAA as "meet the rule, keep the documents." That approach can produce formal compliance while risk grows in the background. Peer-reviewed research shows healthcare breaches are increasing and are heavily driven by hacking/IT incidents and operational realities, rather than missing written policies (Seh *et al*., 2020). Research on ransomware further shows frequent operational disruption, including electronic system downtime and delays or cancellations of care, which transforms cybersecurity into a patient safety issue (Neprash *et al*., 2022). A governance model is meant to stop the pattern where everyone assumes "IT/security is handling it," until an outage forces executive attention. In this framework, HIPAA becomes the "minimum legal baseline," but governance determines whether that baseline is consistently enforced and improved. This aligns with work arguing that healthcare needs stronger resilience and adaptive capacity as systems digitize and interconnect (Garcia-Perez *et al*., 2023). It also aligns with evidence that protecting health records requires thinking beyond basic rule compliance and focusing on how protection is managed and enforced in practice (Subramanian *et al*., 2024).

Core governance principles

This framework rests on four principles. Each one fixes a specific failure mode that shows up repeatedly in healthcare incidents.

Accountability'

Accountability means every HIPAA safeguard has a real owner, and that owner has the authority to make decisions. Ownership without authority is fake accountability. In healthcare breaches, the problem is often not that nobody knew what HIPAA required. The problem is that nobody had a clear responsibility to enforce the requirement when it conflicted with cost, speed, clinician convenience, or vendor pressure (Jalali & Kaiser, 2018). Ransomware evidence shows response outcomes depend on organizational capacity and decisions, not only on the existence of technical controls. For example, Neprash *et al*. (2022) report that only about 1 in 5 organizations were reportedly able to restore data from backups across the attacks they studied, and many incidents disrupted care delivery (Neprash *et al*., 2022). Those are governance outcomes because they reflect prepared decisions made earlier, like backup strategy, testing discipline, and who funded resilience. So, in this model, accountability is built like this: a named owner is assigned for each safeguard area, risk acceptance is controlled so that if a safeguard is weak, someone must either fund the fix or formally accept the risk at the right executive level, and repeated noncompliance triggers escalation rather than a quiet workaround.

Transparency

Transparency means leaders can see the real situation in a language they can act on. That includes what is compliant, what is not, what is risky, and what is trending worse. A major reason HIPAA can fail in practice is that compliance reporting becomes "green dashboards" that hide operational exposure. Transparency fixes that by requiring risk reporting that is tied to HIPAA safeguards and operational consequences: downtime risk, patient safety risk, financial risk, and regulatory risk (Garcia-Perez *et al*., 2023). This is especially important for third-party exposure. A large peer-reviewed survey of healthcare delivery organizations found major visibility gaps in third-party access: only 51.1% reported having a comprehensive inventory of all third parties accessing their network, and 60% said third-party access to sensitive information was not routinely monitored (Gellert & Borgasano, 2025). If leadership cannot see the vendor access reality, it cannot govern it. So, transparency in this framework means reporting focuses on the top operational exposures, not only policy completion; third-party access is made visible through inventory coverage, monitoring coverage, and privileged access control status; and incident lessons are reported as governance failures as well as technical failures.

Risk ownership

Risk ownership means cyber risk is owned as a business and clinical risk, not parked inside IT or compliance. HIPAA requires risk analysis, but that requirement often collapses into periodic checklist activity. Risk ownership fixes this by forcing every major HIPAA-relevant risk to have an "enterprise owner." That owner is typically a senior leader, depending on what is at stake. The security team supports and advises, but ownership sits where decisions and tradeoffs happen (Antonioua, 2018). This principle is not abstract. Third-party breaches and ransomware show that healthcare risk is often created outside the security team's direct control. In the third-party access survey, more than half of respondents reported a breach involving a third party in the prior 12 months, and "lack of oversight or governance" was identified as a barrier by 53% (Gellert & Borgasano, 2025). That

Publisher: SARC Publisher

kind of risk cannot be solved by tools alone. It needs an owner who can enforce vendor requirements, centralize vendor governance, and fund monitoring.

Continuous oversight

Continuous oversight means HIPAA enforcement happens continuously, not only during audits or right after incidents. Healthcare systems change daily: new clinics are acquired, new vendors connect, new cloud services appear, and staff rotate. A yearly compliance cycle cannot keep up with that. Continuous oversight converts HIPAA from a periodic assessment into a living control system (McLeod & Dolezel, 2018). Ransomware evidence shows why this is needed. Attacks increased and grew in impact, and many incidents were reported late relative to statutory timelines, suggesting process and oversight weaknesses (Neprash *et al*., 2022). Continuous oversight makes late detection and late reporting less likely by requiring routine review of incident readiness, monitoring coverage, and escalation performance. This principle also supports resilience thinking in healthcare digital transformation, where adaptive and absorptive capacity are required for long-term security (Garcia-Perez *et al*., 2023). In practical terms, oversight means monthly or quarterly governance routines that review open HIPAA-related risks and their owners, control exceptions and why they were approved, vendor access posture and monitoring coverage, and incident response readiness and tested recovery capability.

Table 1. Governance layers mapped to HIPAA safeguards (illustrative enforcement mapping)

Governance layer	Administrative safeguards (HIPAA)	Physical safeguards (HIPAA)	Technical safeguards (HIPAA)
Board oversight	Sets risk tolerance; requires proof of risk analysis and readiness; reviews breach trends and response performance	Requires capital planning for facility and device security; ensures exceptions are governed	Requires executive assurance for access control and monitoring performance; ensures cyber is treated as enterprise risk
Executive leadership	Owns risk decisions; approves funding; enforces training, incident readiness, vendor governance	Owns asset governance (devices, endpoints, clinical systems); enforces exception handling	Owns identity and access governance; approves standards like MFA, privileged access, logging; sets escalation thresholds
Operational governance (security + IT + compliance)	Runs risk analysis workflows; tracks corrective actions; manages incident governance; runs third-party oversight routines	Implements device and facility control processes; manages inventory and disposal governance	Implements and monitors access controls, audit logging, encryption, segmentation, and detection; reports KPI trends upward

What this mapping tells you is simple: HIPAA compliance fails when these layers are missing or disconnected. When the board does not ask for evidence, executives do not own risk, and operations are left to "do their best," HIPAA turns into documentation rather than enforcement. Vendor exposure makes this worse because third-party access is cross-boundary by nature and needs executive decision authority and continuous monitoring to be governed effectively (Gellert & Borgasano, 2025). Ransomware adds urgency because cyber incidents disrupt care delivery and require fast, high-stakes decisions that cannot be improvised during a crisis (Ogunsola *et al*., 2025).

PROPOSED GOVERNANCE MODEL

This section expands the earlier discussion into a structured governance model designed for HIPAA-regulated healthcare environments. While section 4 explains *why* governance is the missing layer, this chapter explains *how* healthcare organizations can structure, operate, and enforce governance so that HIPAA compliance actively reduces cybersecurity risk. Governance models are not new in cybersecurity. However, most existing models are either generic enterprise frameworks or technology focused operating models. Healthcare presents a different problem space. Clinical uptime, patient safety, regulatory exposure, and deep reliance on third parties create risk dynamics that cannot be managed through technical controls alone. The proposed model, therefore, treats governance as an operational system that links leadership decision making, compliance enforcement, and day-to-day security execution.

Publisher: SARC Publisher

Governance Structure

The governance structure defines where authority sits, how oversight is exercised, and how accountability flows. Without structure, governance collapses into informal coordination and ad hoc decisions. The proposed governance model sets clear roles at three levels. At the top, the board provides enterprise risk oversight for cybersecurity and HIPAA by treating cyber risk as a standing agenda item and focusing on whether key risks are understood, resourced, and being corrected when governance failures appear (Antoniou, 2018). Next, a formal executive cybersecurity and compliance committee turns board expectations into enforceable decisions by prioritizing risk, approving risk acceptance, allocating funding, and resolving conflicts between operational convenience and HIPAA safeguards, since delayed executive decisions can worsen breach impact and downtime, especially in ransomware events (Ogunsola *et al*., 2025; Neprash *et al*., 2022). Finally, compliance and security are integrated through dedicated roles that translate HIPAA requirements into enforceable controls, track deviations, and escalate gaps, addressing the documented mismatch between audit success and real-world breach outcomes (Seh *et al*., 2020; Subramanian *et al*., 2024).

Policy and Decision Framework

Governance is ineffective without clear rules for how decisions are made and enforced. The policy and decision framework defines how HIPAA requirements influence everyday choices. The proposed model strengthens enforcement through three linked mechanisms. First, policy enforcement is risk-based rather than static, so high-risk assets and workflows get stricter controls and faster remediation, reflecting evidence that common healthcare breach drivers include credential misuse, unmonitored third-party access, and delayed patching (Seh *et al*., 2020; Gordon *et al*., 2021). Second, it uses defined escalation mechanisms so unresolved HIPAA safeguard gaps move up a set path from operational teams to executives and, if needed, the board, reducing silent risk acceptance and improving containment outcomes that are often worse when escalation is unclear (Bonsu & Opoku, 2025; Neprash *et al*., 2022). Third, it embeds third-party governance into enterprise decision-making by treating vendor access to PHI systems as an ongoing risk that requires approval, monitoring, and periodic review, responding to evidence of major monitoring gaps and vendor-related exposure in healthcare organizations (Gellert & Borgasano, 2025).

Operational Alignment

Governance only matters if it shapes operations. This section explains how governance connects to audits, monitoring, and incident response. The model ties governance to execution through three practices. First, audits are reframed as governance feedback, so repeated findings, delayed remediation, or control failures trigger governance review rather than superficial corrective action plans, addressing evidence that audit success does not reliably predict real security resilience (Seh *et al*., 2020). Second, it replaces episodic compliance checks with continuous compliance monitoring focused on control performance, exception trends, and risk exposure over time, reported to executives in a consistent decision-ready format, which supports the adaptive governance linked to resilience in digitally transforming healthcare systems (Garcia-Perez *et al*., 2023). Third, incident response is treated as a governance process with pre-defined roles, decision authority, and communication responsibilities, and post-incident reviews assess governance failures alongside technical causes, reflecting findings that ransomware outcomes depend heavily on preparedness, leadership engagement, and decision speed (Neprash *et al*., 2022).

Governance-to-Compliance Mapping

The final component of the model shows how governance mechanisms enforce HIPAA safeguards in practice. Governance controls act as enforcement levers. Administrative safeguards are enforced through accountability, risk ownership, and oversight. Physical safeguards are enforced through asset governance, access approval, and exception management. Technical safeguards are enforced through standards, monitoring, and escalation authority. Boards are accountable for oversight, executives are responsible for enforcement decisions, compliance and security teams are responsible for implementation and monitoring, and operational staff are informed and trained. This clarity prevents the diffusion of responsibility that characterizes many breach-prone organizations.

Governance metrics and key performance indicators focus on behavior and outcomes rather than artifacts. Metrics include risk ownership coverage, escalation timeliness, vendor monitoring coverage, and incident containment time. These indicators reflect governance performance rather

Publisher: SARC Publisher

than mere policy existence. Finally, the model supports compliance maturity progression. Organizations move from reactive compliance, where HIPAA is treated as a legal checkbox, to managed compliance, where governance enforces safeguards consistently, and ultimately to adaptive compliance, where governance anticipates risk and continuously improves protection. Literature on healthcare cybersecurity maturity supports this progression and links higher governance maturity to improved resilience and reduced incident impact (Garcia-Perez *et al*., 2023). This governance model provides a practical bridge between HIPAA requirements and cybersecurity outcomes. It shows how leadership structures, decision frameworks, and operational alignment can transform compliance from a static obligation into an active risk management system. By making governance the enforcement engine of HIPAA, the model addresses the root causes of persistent healthcare breaches identified throughout.

EVALUATION METRICS AND VALIDATION APPROACH

In healthcare cybersecurity, effectiveness cannot be inferred from policy existence, audit completion, or formal compliance status. Empirical evidence shows that organizations experiencing major breaches were often HIPAA compliant at the time of the incident, which means evaluation must focus on governance performance and risk reduction rather than compliance formality alone (Seh *et al*., 2020; Subramanian *et al*., 2024).

The evaluation framework for this study is therefore designed to answer a single overarching question: Does compliance-driven cybersecurity governance measurably reduce risk exposure and improve security outcomes in HIPAA-regulated environments? To answer this, the evaluation must consider governance behavior, compliance enforcement quality, operational risk exposure, and downstream breach and audit outcomes as a connected system.

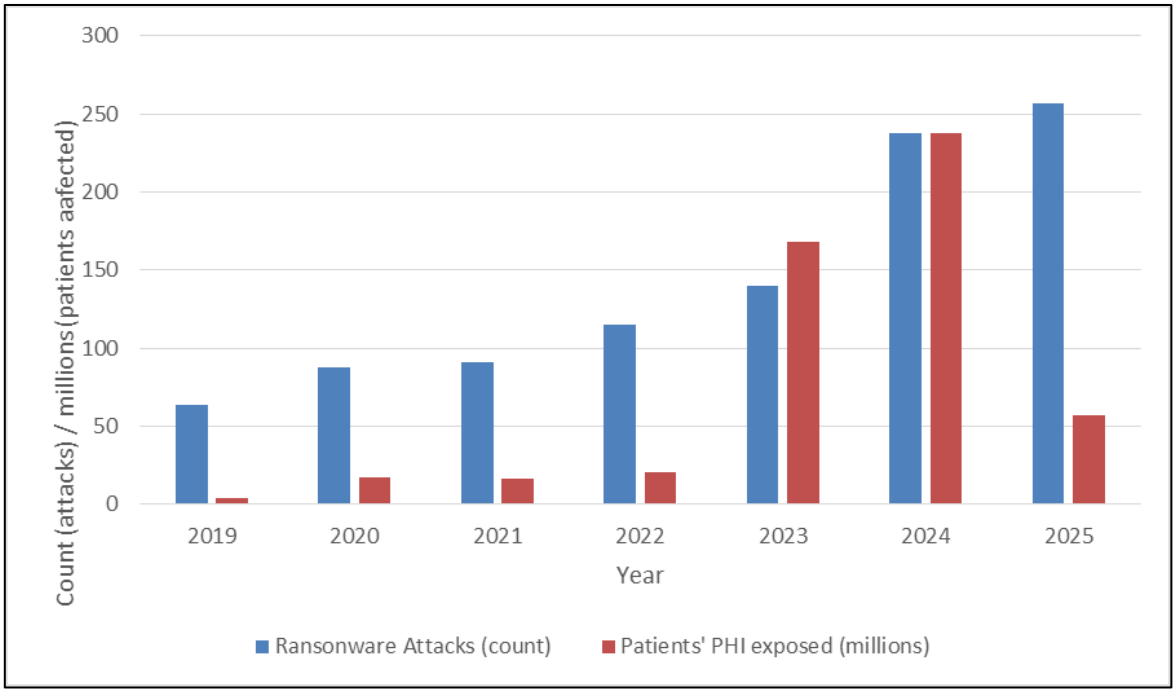

Figure 2: Escalation of Ransomware Incidents and Patient Data Exposure in U.S. Healthcare.

In Figure 2, we illustrate the sharp escalation in both ransomware attacks and the volume of exposed patient health information (PHI) across the healthcare sector over recent years. The trend shows that ransomware incidents have increased significantly, from 64 attacks in 2019 to 257 in 2025, while the number of affected patient records has also risen, with notable spikes such as 237.9 million exposed records in 2024. These patterns highlight how healthcare systems continue to experience growing operational and privacy impacts despite regulatory requirements, underscoring the need for stronger governance, faster detection, and continuous monitoring to reduce breach severity and exposure duration

Governance effectiveness indicators

Governance effectiveness is evaluated by observing whether leadership oversight,

Publisher: SARC Publisher

accountability, and decision authority function as intended over time. Effective governance is reflected in how quickly risks are identified, owned, and acted upon, rather than how often policies are reviewed. Indicators of governance effectiveness, therefore, focus on decision dynamics rather than technical controls. One core indicator is risk ownership completeness, measured by the proportion of high-risk HIPAA-related findings that are assigned to named executive owners. Persistent unowned risks signal governance failure because unresolved exposure remains outside formal accountability. Another indicator is decision timeliness, which captures the elapsed time between risk identification and an executive-level decision to mitigate, accept, or transfer that risk. Studies of healthcare ransomware incidents show that delays in leadership decision-making contribute directly to prolonged downtime and increased clinical disruption, making decision speed a critical governance metric (Neprash *et al*., 2022). Governance effectiveness is also reflected in exception behavior. Frequent or long-lived exceptions to security controls indicate that governance is permitting deviations without adequate justification or oversight. Over time, a high exception burden correlates with higher incident likelihood because controls exist in theory but not in practice. Finally, board-level engagement is evaluated by the regularity and consequence of cybersecurity review. Board oversight that does not result in reprioritization, funding adjustments, or corrective action is functionally ineffective, even if meetings occur (Zhang *et al*, 2021).

Reduction in compliance gaps

Reduction in compliance gaps is assessed by examining whether HIPAA safeguard deficiencies decrease in frequency, severity, and recurrence. Unlike traditional compliance measurement, which emphasizes audit pass rates, this approach evaluates whether identified gaps are resolved and remain resolved. A meaningful reduction in compliance gaps is observed when remediation timelines shorten, repeated findings decline across audit cycles, and corrective actions are supported by operational evidence rather than documentation alone. Research shows that recurring compliance findings are a strong signal of weak governance enforcement, because the organization has knowledge of deficiencies but lacks the authority or incentive to correct them (Seh *et al*., 2020). In a governance-driven model, repeated findings are treated as governance failures rather than operational oversights, triggering escalation and review at higher decision levels. Over time, effective governance should produce fewer material compliance gaps, faster remediation, and greater consistency between documented safeguards and observed system behavior. These changes indicate that compliance has shifted from a reporting exercise to an enforced operational requirement.

Risk exposure metrics

Risk exposure metrics measure the organization's current vulnerability to cybersecurity incidents, independent of audit cycles. These metrics focus on conditions that empirical research has repeatedly linked to healthcare breaches, including third-party access, identity and access management, vulnerability persistence, and preparedness for ransomware-related disruption (Seh *et al*., 2020; Neprash *et al*., 2022). In healthcare environments, third-party access represents one of the most significant sources of systemic risk. Recent peer-reviewed survey research shows that many healthcare organizations lack comprehensive visibility into which vendors access sensitive systems and do not routinely monitor that access, while a majority report experiencing third-party-related breaches within one year (Gellert & Borgasano, 2025). Governance effectiveness is therefore reflected in whether vendor access is inventoried, monitored, and reviewed as a continuous governance function rather than a one-time contracting activity. Risk exposure is also reflected in how long critical vulnerabilities remain unpatched, how widely privileged access is distributed, and whether backup and recovery capabilities are tested under realistic conditions. Ransomware studies demonstrate that the ability to restore systems and resume care depends on governance decisions made long before an incident occurs, such as investment in backup infrastructure and enforcement of recovery testing (Neprash *et al*., 2022). Declining exposure across these dimensions indicates that governance is influencing operational risk posture rather than merely overseeing compliance artifacts.

Audit quality improvements

Audit quality improvement is evaluated by whether audits become more predictive of real-world security risk. Traditional HIPAA audits often emphasize policy existence and procedural documentation, which has limited value for breach prevention. Governance-driven audits shift focus

Publisher: SARC Publisher

toward operational evidence and enforcement capability. Improved audit quality is reflected in greater reliance on system-generated evidence, such as access logs, monitoring outputs, and configuration data, rather than written attestations. It is also reflected in stronger alignment between audit findings and known breach drivers. For example, audits that consistently identify weaknesses in vendor access monitoring, privilege management, or incident readiness are more likely to surface meaningful risk than audits focused on training records or policy language (Eoyand & Keitner, 2020). From a governance perspective, audit quality improves when audit outcomes drive executive action rather than routine corrective action plans. When audit findings lead to funding decisions, structural changes, or leadership accountability, audits become governance instruments rather than compliance rituals. Research on healthcare security emphasizes that protection beyond HIPAA requires this kind of operational verification and leadership engagement (Subramanian *et al*., 2024).

Proposed validation approach using breach and audit data

Validation of the proposed governance model requires demonstrating a relationship between governance implementation and measurable changes in risk exposure and security outcomes. This study proposes a multi-method validation approach using both internal organizational data and external breach datasets. Internally, longitudinal data on governance indicators, compliance gaps, risk exposure metrics, and audit findings can be analyzed before and after governance model adoption. An interrupted time-series approach allows assessment of whether trends in exposure and incidents change following implementation, rather than relying on single-point comparisons. This approach is particularly suitable for healthcare organizations where randomization is not feasible (Zhang *et al*., 2021). Externally, publicly available breach data from the HHS Office for Civil Rights can be used to contextualize observed changes against industry-wide trends. If organizations implementing governance-driven compliance show greater reductions in breach frequency or severity relative to sector averages, this strengthens causal inference. Prior studies using OCR data demonstrate that breach patterns are sufficiently stable to support comparative analysis over time (McLeod & Dolezel, 2018; Seh *et al*., 2020). The critical validation logic is sequential. Governance improvements should first appear as better risk ownership and faster decisions, then as reduced exposure metrics, and finally as improved incident and audit outcomes. This causal chain reflects how governance operates in practice and avoids the false assumption that compliance alone directly prevents breaches.

FUTURE RESEARCH DIRECTIONS

This study proposes a compliance-driven cybersecurity governance model for HIPAA-regulated healthcare systems. The model is designed to address the gap between formal compliance and real security outcomes by strengthening accountability, oversight, and operational enforcement. The next step for the research community is to test, refine, and extend the model using empirical evidence, new analytic methods, and broader comparisons. This section outlines three future research directions that can strengthen the scientific foundation of governance-driven HIPAA cybersecurity.

Empirical testing of governance models

The most immediate research need is empirical testing of the proposed governance model in real healthcare settings. Much of the current literature establishes that breaches persist despite compliance, but fewer studies measure whether specific governance structures reduce risk over time (Seh *et al*., 2020; Subramanian *et al*., 2024). Future work should move beyond conceptual proposals and examine measurable outcomes such as reduced policy exceptions, improved remediation speed, stronger third-party oversight, and lower incident severity. A strong design would test whether governance changes alter risk exposure before they alter breach outcomes. This is important because breach outcomes are noisy and affected by external threat levels, while governance indicators and exposure metrics reflect internal control. Researchers can evaluate governance model adoption using interrupted time-series designs, matched comparisons between early and late adopters, or multi-site studies within hospital systems. The empirical goal should not be to prove that governance "stops" attacks, but to show that governance reduces the likelihood of high-impact incidents and improves containment and recovery when incidents occur. Evidence from ransomware research shows that impact is heavily tied to organizational readiness and response capacity, which can directly influence (Neprash *et al*., 2022). A second empirical gap is third-party governance. Since healthcare depends on vendors

Publisher: SARC Publisher

for cloud services, revenue cycle management, data exchange, and clinical platforms, future research should test whether governance mechanisms such as continuous access monitoring, contractual enforcement, and centralized vendor risk ownership reduce breach propagation across organizations. Recent peer-reviewed survey data suggests many healthcare organizations still lack comprehensive third-party visibility and routine monitoring, making this a high-value area for testing governance interventions (Gellert & Borgasano, 2025).

AI-supported compliance governance

Another promising direction is the use of AI to support continuous compliance governance. Many compliance failures occur because risk signals are scattered across systems, teams, and vendors. AI methods can help by consolidating evidence, detecting patterns, and highlighting governance breakdowns earlier than periodic reviews would. Future studies can explore AI-assisted compliance evidence collection, where models extract and classify control evidence from logs, configuration snapshots, ticketing systems, and vendor attestations. This approach can reduce the documentation burden while improving audit evidence quality. AI can also support exception governance by detecting repeated exception patterns, identifying controls that are routinely bypassed, and flagging risk decisions that lack appropriate approvals. A high-impact research theme is governance-focused AI explainability. In healthcare, leaders must justify risk decisions to regulators and boards. AI systems that offer risk scoring without a clear rationale will face resistance. Research should therefore focus on transparent decision support tools that link AI outputs to HIPAA safeguards and governance decision points, rather than treating AI as a black box. This aligns with recent research emphasizing that healthcare cybersecurity improvement requires operational enforcement and verifiable evidence, not only policy statements (Subramanian *et al*., 2024).

Longitudinal governance impact studies

Finally, longitudinal studies are necessary to understand whether governance improvements are sustained and whether they meaningfully change breach outcomes over time. Governance is not a one-time intervention. It is an ongoing system of oversight, accountability, and enforcement. Short-term studies may capture early improvements in visibility and compliance, but only long-term observation can show whether those improvements persist and translate into measurable outcome changes. Longitudinal research should track governance indicators, risk exposure metrics, audit quality measures, and incident outcomes for multiple years. Ransomware trends show that healthcare cyber risk evolves over time and can increase rapidly, which means governance must remain adaptive rather than static (Neprash *et al*., 2022). Longitudinal studies can also capture delayed effects, such as how governance changes influence procurement decisions, system modernization, vendor selection, and staff security culture, all of which may take years to produce measurable breach reduction. A valuable longitudinal focus is the relationship between vendor ecosystem governance and systemic breach exposure. Since breaches increasingly involve interconnected entities, researchers should examine whether governance maturity at one organization reduces risk only locally or also reduces downstream exposure across partner networks. This moves governance research from a single-organization perspective to a healthcare ecosystem perspective, which better reflects real-world risk.

CONCLUSION

This study shows that cybersecurity failures within HIPAA-regulated healthcare environments persist not because the law does not have enough protection, but because the governance systems responsible for enforcing those safeguards are inconsistently implemented. Recent trends in healthcare breaches show that both frequency and impact of cyberattacks in healthcare continue to increase, even among organizations that formally comply with regulatory requirements. Evidence suggests that these failures are frequently associated with weak execution, unclear accountability structure, and insufficient third-party governance.

By reframing HIPAA compliance as a governance problem rather than a technical or documentation exercise, this paper identifies governance as the missing layer between regulatory intent and operational security outcomes. The proposed compliance-driven cybersecurity governance model integrates board-level oversight, executive decision authority, compliance-security coordination, and continuous enforcement into a unified structure aligned with HIPAA safeguards. In contrast to conventional methods, we place a strong emphasis on escalation discipline, accountability, risk ownership, and quantifiable

Publisher: SARC Publisher

governance performance. By focusing on governance behavior and enforcement capability rather than solely on technical control deployment, this study contributes to the advancement of healthcare cybersecurity research. The findings highlight the need for stronger governance that ensures existing regulations are implemented effectively, rather than more regulations, for researchers, regulators, and healthcare leaders.

REFERENCES

1. Agarwal, K., & Shah, M. "The Role of Corporate Governance in Managing Cybersecurity Risks: A Comprehensive Analysis." *LawFoyer Int'l J. Doctrinal Legal Rsch.* 2 (2024): 352.
2. Ahmed, Z., Filani, A., Osifowokan, A. S., & Hutchful, N. "The Impact of Data Breaches in US Healthcare: A Cost-Benefit Analysis of Prevention vs. Recovery." (2025).
3. Alla, S., Komaragiri, S. G., Duvall, T., Karahan, S., Bheesetty, N., & Chattu, V. K. "A Governance-Centric Framework for Strengthening Healthcare Cybersecurity: A Systems Perspective." *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, (2025).
4. Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. "An exploratory study of current information security training and awareness practices in organizations." (2018).
5. Antoniou, G. S. "A Framework for the Governance of Information Security: Can it be Used in an Organization." *SoutheastCon 2018*. IEEE, (2018).
6. BankInfoSecurity. "2025 in health data breaches and predictions for 2026". (2025).
7. Bonsu, M. A., & Opoku, J. A. "Privacy Challenges in IoT: Assessing Data Protection Risks and Strategies for Secure User Adoption." (2025).
8. CISA. "Cybersecurity incident response guide for the healthcare and public health sector." *Cybersecurity and Infrastructure Security Agency*. (2023).
9. Eoyang, M., & Keitner, C. "Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity." *J. Nat'l Sec. L. & Pol'y* 11 (2020): 327.
10. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. "Resilience in healthcare systems: Cyber security and digital transformation." *Technovation* 121 (2023): 102583.
11. Gellert, G. A., Borgasano, D., Palermo, R., Gellert, G. L., & Kelly, S. P. "Third-party access cybersecurity threats and precautions: a survey of healthcare delivery organizations." *Applied Clinical Informatics* 16.05 (2025): 1518-1530.
12. Gordon, W. J., Fairhall, A., & Landman, A. "Threats to information security—public health implications." *N Engl J Med* 377.8 (2017): 707-709.
13. HIPAA Journal. "Largest healthcare data breaches of 2025". (2026).
14. Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. "Measurement models of information security based on the principles and practices for risk-based approach." *Procedia Manufacturing* 44 (2020): 647-654.
15. IBM Security & Ponemon Institute. "Cost of a data breach report 2024." (2024).
16. Jalali, M. S., & Kaiser, J. P. Jalali, M. S., & Kaiser, J. P. "Cybersecurity in hospitals: a systematic, organizational perspective." *Journal of medical Internet research* 20.5 (2018): e10059.
17. Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. "Why employees (still) click on phishing links: investigation in hospitals." *Journal of medical Internet research* 22.1 (2020): e16775.
18. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. "Cybersecurity in healthcare: A systematic review of modern threats and trends." *Technology and Health Care* 25.1 (2017): 1-10.
19. McLeod, A., & Dolezel, D. "Cyber-analytics: Modeling factors associated with healthcare data breaches." *Decision Support Systems* 108 (2018): 57-68.
20. Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., & Nikpay, S. S. "Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021." *JAMA Health Forum*. 3. 12. (2022).
21. Ogunsola, O., Adikorley, I. J. N., & Opoku, J. A. "Mitigating Cognitive Load in Supply Chain Decision-Making: An AI-Driven Framework for Enhanced Operational Efficiency."
22. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. "Healthcare data breaches: insights and

Publisher: SARC Publisher

implications." *Healthcare*. Vol. 8. No. 2. MDPI, (2020).
23. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. "Healthcare data breaches: insights and implications." *Healthcare*. Vol. 8. No. 2. MDPI, (2020).
24. Singh, A. "From past to present: the evolution of data breach causes (2005–2025)." *LatIA* 3 (2025): 333-333.
25. Subramanian, H., Sengupta, A., & Xu, Y. "Patient health record protection beyond the health insurance portability and accountability Act: mixed methods study." *Journal of medical Internet research* 26 (2024): e59674.
26. Verizon. "2024 Data Breach Investigations Report: Healthcare snapshot." *Verizon*. (2024).
27. Viswanathan, V. S., Harri, P., Volin, J., Kadakia, J., Safdar, N., & Kikano, E. "Best Practices in Cybersecurity Governance: Safeguarding Radiology." *Journal of the American College of Radiology* 22.10 (2025): 1132-1140.
28. Zhang, L., Wattal, S., & Pang, M. S. "Does sharing make my data more insecure? An empirical study on health information exchange and data breaches." *MIS Quarterly* 48.3 (2024): 873-898.
29. Zhang, R., Xue, R., & Liu, L. "Security and privacy for healthcare blockchains." *IEEE Transactions on Services Computing* 15.6 (2021): 3668-3686.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Addotey, N. "Designing Compliance-Driven Cybersecurity Governance Models for Hipaa-Regulated Healthcare Systems" *Sarcouncil Journal of Engineering and Computer Sciences* 5.4 (2026): pp 83-94.

Publisher: SARC Publisher