FPT UNIVERSITY

MINISTRY OF EDUCATION AND TRAINING

FPT UNIVERSITY

Capstone Project Document

Developing an Automated System to Monitor Compliance with Electronic Health Record (EHR) Security Policies in Small and Medium-Sized Healthcare Facilities

Group Member	**Student's name**	**Student's ID**
	Tran Gia Quy	DA170010
	Nguyen Khanh Toan	DE170585
	Nguyen Xuan Hoang	DE170316
	Nguyen Khanh Linh	DE170403
	Nguyen Huu Khoi	DE170017
Supervisor	**Supervisor's Name**	
	Nguyen Van Dien	
	Pham Ho Trong Nguyen	
Capstone Project code	IAP491	

- Hanoi, Sep/2025 -

ABSTRACT

Background: Electronic Health Records (EHRs) are quickly becoming more common in Vietnam's small and medium-sized healthcare facilities. This is because of national digital health programs and stronger rules for protecting personal data. But these facilities have a hard time showing that they follow security rules because they don't have enough technological resources, their permission systems are broken, and they don't have any automated monitoring systems. Current methods depend too much on manual audits and reactive investigations, which aren't enough to show that every access to sensitive health data is legal, essential, purpose-bound, and able to be audited.

Methods: This study creates an architecture that combines identity and access control, electronic medical record workflows, and automated compliance monitoring. Keycloak is used for centralized authentication, NGINX is used as a policy enforcement point that asks Open Policy Agent for real-time authorization decisions, FastAPI is used as the core of the EHR for managing clinical data, and a Security Information and Event Management (SIEM) backend automatically checks logs against compliance rules based on Vietnamese legal requirements. The evaluation method uses a "Red Team vs. Blue Team" simulation to test the system against three important attack scenarios: Brute-Force Authentication, SQL Injection, and Forensic Trace Deletion (Log Tampering).

Results: The system was able to stop Brute-Force and SQL Injection attacks at the Identity and Gateway layers, respectively. In the Log Tampering scenario, the system's hash-chain integrity mechanism found that someone had deleted audit trails without permission, which set off a critical warning. These results show that a layered defense architecture may effectively enforce compliance and keep evidence integrity without using hidden statistical anomaly detection.

Conclusions: The proposed system effectively translates Vietnamese regulatory requirements into implementable technical controls and offers automated, auditable compliance monitoring tailored for resource-limited healthcare facilities. The architecture shows that it is possible for small and medium-sized providers to do this while still keeping patient safety and clinical productivity high. In the future, work should focus on increasing rule coverage, making it easier to find complicated violation patterns, and meeting compliance criteria in more than one jurisdiction for international deployment.

Keywords: Electronic Health Records, Compliance Monitoring, Security Policies, Healthcare Facilities, Automated Auditing, Policy Enforcement, Access Control

ACKNOWLEDGEMENT

We would like to express our deepest gratitude to all those who have contributed to the successful completion of this thesis.

First and foremost, we extend our sincere appreciation to our thesis supervisors, Dr. Nguyen Van Dien and Dr. Pham Ho Trong Nguyen, for their invaluable guidance, continuous support, and insightful feedback throughout this research. Their expertise in information security and healthcare informatics has been instrumental in shaping our work, from the initial problem formulation through to the final system implementation and evaluation.

Throughout this journey, they provided invaluable insights that helped us navigate the complexities of healthcare compliance monitoring, policy enforcement mechanisms, and system architecture design. Their constructive feedback on both the technical implementation and the written presentation of this work significantly improved the quality and clarity of the thesis. We are particularly grateful for their patience and encouragement during the most challenging phases of system development, when debugging integration issues between multiple components, refining the evaluation methodology, and ensuring that the system met both functional and compliance requirements demanded persistent problem-solving and attention to detail.

Their ability to ask the right questions and guide us toward finding solutions has not only enriched this research but also deepened our understanding of the field and improved our skills as researchers and developers.

This thesis would not have been possible without the collective effort and support of everyone involved. The journey from initial concept to final implementation has been both challenging and rewarding, and we are truly grateful for the guidance, encouragement, and expertise that have been shared with us throughout this process. Thank you all for being part of this journey with us.

TABLE OF CONTENTS

ABBREVIATIONS

Acronym	Meaning
API	Application Programming Interface
EHR	Electronic Health Record
IAM	Identity and Access Management
JSON	JavaScript Object Notation
JWT	JSON Web Token
KPI	Key Performance Indicator
MTTD	Mean Time To Detect
MTTR	Mean Time To Respond
OPA	Open Policy Agent
PEP	Policy Enforcement Point
PDP	Policy Decision Point
PIPEDA	Personal Information Protection and Electronic Documents Act
RBAC	Role-Based Access Control
REST	Representational State Transfer
SIEM	Security Information and Event Management
SSO	Single Sign-On
TLS	Transport Layer Security

Table 1 – *List of Acronyms*

CHAPTER 1 - INTRODUCTION

(Provides background information, introduces the research problem, and outlines the purpose and significance of the study.)

1.1. Background

Vietnam's healthcare sector is undergoing rapid digital transformation, with electronic health record (EHR) systems increasingly adopted across hospitals and clinics. Recent estimates report that more than 93% of hospitals in Ho Chi Minh City have deployed EHR systems, indicating strong momentum toward digital health operations. [4] To sustain this transformation, healthcare providers—especially small and medium-sized facilities—must adapt to tightening data protection and compliance expectations. [25], [30]

However, rapid digitization does not automatically translate into strong security and compliance. In resource-limited environments, security controls often lag behind adoption due to budget, staffing, and infrastructure constraints, increasing the risk of patient data exposure. In many facilities, authorization is fragmented across multiple applications (HIS, EHR portals, imaging, laboratory, billing), monitoring remains reactive, and audit evidence is not strong enough to support high-confidence investigations or regulatory reporting. [5]

Prior research and systematic reviews have highlighted that healthcare compliance monitoring remains a global challenge due to the complexity of privacy regulations and the lack of automated, operationally feasible auditing mechanisms—especially when systems are heterogeneous and resources are constrained. Beyond purely technical enforcement, healthcare environments must also consider workflow usability: controls that introduce excessive friction can degrade clinical productivity or trigger workarounds, particularly in urgent care. [26], [17], [18]

Therefore, this thesis focuses on a practical, measurable compliance monitoring approach that strengthens accountability for EHR access while remaining feasible for small and medium-sized healthcare facilities in Vietnam under real operational constraints. [5]

1.2. Problem Statement

1.2.1 Current Operational Gaps (Pain Points)

Despite increasing EHR adoption, many small and medium-sized healthcare facilities in Vietnam lack a centralized, lightweight, and reliable mechanism to ensure—and prove—that every EHR access is lawful, necessary, accountable, and auditable under operational constraints. [5], [26]

Key pain points are summarized as follows.

(G1) Fragmented authorization without a unified checkpoint.
Access control is often implemented separately across systems, leading to inconsistent policy enforcement and delayed or incomplete revocation when staff change roles or leave. This makes

it difficult to enforce context-based restrictions (department, shift/on-call status, network zone, device type) consistently across all access paths. [5]

(G2) Weak binding of "purpose of use" and consent to the access session.
In practice, many workflows do not require users to declare a purpose for each access session (e.g., treatment, billing, administration, training), and consent validation may not be consistently enforced at access time. This undermines purpose limitation and reduces the ability to justify access during audits or disputes. [2], [26]

(G3) Monitoring remains reactive and correlation is limited.
Logs are often reviewed after incidents instead of being used for early detection of misuse. A common limitation is the lack of standardized correlation identifiers across layers (gateway/application/database), which prevents building a complete end-to-end narrative of access behavior. [17], [18]

(G4) Audit evidence integrity is insufficient for high-confidence investigations.
Audit logs may be incomplete due to rotation, deletion, time drift, or inconsistent collection across systems. Without robust integrity measures, evidence can be challenged or become unreliable for audits and incident reconstruction. [17], [18]

(G5) Resource constraints hinder sustainable operations.
Small IT teams and constrained infrastructure make heavyweight monitoring solutions difficult to deploy and maintain. Excessive alert noise can cause fatigue, while outages (power/network) can disrupt logging and monitoring continuity. [5]

1.2.2 Consequences if Unresolved

If these gaps remain unresolved, facilities face escalating risks:

Regulatory and legal exposure: inability to demonstrate compliance with purpose limitation, consent handling, and accountability expectations for sensitive health data. [2], [25], [30]

Operational risk: delayed detection of misuse, slow investigations, and weak evidence chains. [17], [18]

Clinical risk through poor UX design: if access controls introduce significant friction (e.g., mandatory "purpose selection" without workflow optimization), clinicians may be slowed in urgent contexts or may adopt unsafe workarounds. [5]

Governance risk: management cannot measure compliance posture reliably or prioritize improvements without consistent metrics and trustworthy evidence. [17], [18]

1.2.3 Desired Capabilities (Target State)

A practical target state for small and medium-sized facilities is a "right-sized" compliance monitoring capability that delivers.

Unified enforcement: route sensitive EHR access through a single checkpoint that evaluates role + attributes + context and records explainable allow/deny decisions. [17], [18]

Human-centrism purpose binding: require purpose declaration in a workflow-friendly manner (fast selection, sensible defaults) and support controlled emergency access ("break-glass") with justification and post-event review. [2], [5]

Standardized, correlated auditing: ensure access events can be linked across systems by consistent identifiers for user, patient, request/session, time, and purpose to support investigations and reporting. [17], [18]

Proactive, low-noise monitoring: detect anomalous access patterns early with measurable detection quality (e.g., precision/recall) and operational response metrics (MTTD/MTTR). [17], [18]

Trustworthy evidence for audits: strengthen audit evidence quality so it remains credible for internal investigation and regulatory reporting. [17], [18]

Feasible deployment and resilience: remain sustainable under limited personnel and infrastructure, including handling degraded operation during outages with clear recovery practices. [5]

1.2.4 Research Questions

Based on the current gaps and desired capabilities, this thesis addresses the following research questions.

RQ1: How can sensitive EHR access be routed through a unified enforcement checkpoint while meeting clinical latency requirements?

RQ2: How can purpose-of-use and consent validation be bound to access sessions without unacceptable operational friction, especially for emergency workflows?

RQ3: How can audit data across system layers be standardized and correlated to enable low-noise, near-real-time detection of misuse?

RQ4: How can audit evidence be made reliable enough for investigations and audits under constrained resources?

RQ5: What KPIs best represent compliance posture and monitoring effectiveness in small and medium Vietnamese healthcare facilities?

1.3 Research Objectives

Electronic Health Records in Vietnam are expanding under national digital health initiatives and tightening personal data protection expectations. This creates a practical requirement for healthcare providers, especially small and medium-sized facilities, to demonstrate that each access to patient data is lawful, purpose-bound, attributable, and auditable. At the same time, these facilities must operate under constraints in staffing, budget, and infrastructure where heavyweight security solutions are often infeasible or unsustainable. [5], [2]

Overall Aim

The overall aim of this thesis is to design, operationalize, and evaluate a practical compliance monitoring approach for EHR access in Vietnam that converts legal and ethical requirements into measurable technical controls and audit-ready evidence while remaining feasible for small and medium-sized healthcare facilities. [2], [5]

Specific Objectives

1.3.1 Translate compliance requirements into testable technical controls

This objective aims to interpret key Vietnamese requirements relevant to EHR management and personal data protection, then express them as testable control statements. The result is a traceable mapping that links each control to a compliance requirement, ensuring the system design is grounded in enforceable obligations rather than informal best-effort rules. [1], [2]

1.3.2 Establish a unified enforcement checkpoint for sensitive EHR access

This objective focuses on consolidating sensitive access paths behind a single enforcement point where authorization decisions are evaluated consistently. Instead of distributing access logic across multiple systems, the checkpoint provides a uniform decision process and records the decision rationale, which improves auditability and reduces policy drift across applications. [17]

1.3.3 Design purpose-aware and consent-aware access with workflow constraints

This objective aims to bind each sensitive access session to a declared purpose of use and verify that access conditions align with that purpose and relevant consent constraints. Importantly, it treats usability as a core constraint: the design must minimize operational friction and support emergency workflows through a controlled break-glass mechanism with justification and post-event review, rather than forcing rigid steps that could disrupt urgent care. [2], [5]

1.3.4 Define a minimal, correlation-ready audit footprint

This objective defines what audit data must be captured at minimum to reconstruct an end-to-end access narrative across heterogeneous systems. It specifies the identifiers required for correlation across layers, such as user identity, patient/resource reference, time, request/session linkage, and

the declared purpose. This makes audit trails investigable and measurable rather than fragmented artifacts that cannot be reliably joined. [17], [18]

1.3.5 Develop monitoring signals and evaluate detection performance

This objective derives monitoring signals from audit trails to identify misuse patterns that are common in healthcare settings, including after-hours access, cross-department viewing, abnormal volume spikes, and suspicious access sequences. The evaluation is designed to report measurable monitoring performance, including timeliness and alert quality, so that "monitoring works" is supported by evidence rather than claims. [18]

1.3.6 Strengthen audit evidence credibility for investigations and reporting

This objective focuses on producing audit evidence that remains trustworthy under realistic operational risks, including log rotation, deletion attempts, and time inconsistencies. The goal is not to claim perfect immutability, but to reach audit-ready credibility by enforcing evidence completeness, integrity validation practices, and operational controls that prevent silent evidence loss. [17]

1.3.7 Produce a compliance scorecard and an evaluation package for stakeholders

This objective translates collected data into indicators that stakeholders can understand and act upon, such as coverage of sensitive access paths through the checkpoint, completeness of purpose binding, correlation integrity, monitoring timeliness, and operational stability. The scorecard is designed to support management reporting and internal governance decisions, while still enabling drill-down to event-level evidence when required. [17]

1.4. Significance of the Study

This study is significant because it addresses a gap that many EHR deployments face in practice: operating EHR systems does not automatically mean a facility can prove accountability and compliance when incidents, disputes, or inspections occur. The challenge is more acute in small and medium-sized healthcare facilities where fragmented systems, limited staffing, and constrained infrastructure reduce the effectiveness of conventional security approaches. [5]

Practical significance for Vietnam's compliance needs

Health data is classified as sensitive personal data, and Vietnamese compliance expectations increasingly emphasize purpose limitation, accountability, and protection of confidentiality. [2] The study supports these needs by converting requirements into operational controls that can be tested, measured, and evidenced. Instead of relying on policy documents and manual log review, the proposed approach strengthens the facility's ability to show why access was allowed, what purpose it served, and what evidence supports that claim when questioned. [17]

Operational significance under resource constraints

A key feature of the proposed approach is its focus on feasibility in constrained environments. Many facilities cannot sustain high-complexity, high-maintenance systems. This study's emphasis on measurable controls, minimal necessary audit data, and operationally realistic monitoring helps reduce false confidence created by incomplete logs or sporadic reviews. It shifts compliance from an aspirational statement to an operational capability. [5]

Human-centric significance in clinical workflows

Healthcare security cannot be evaluated only by "how strict it is." Controls that introduce excessive friction may degrade clinical performance or incentivize workarounds, especially in urgent contexts. This study is significant in explicitly treating purpose binding and emergency access as workflow design problems, aiming to reduce friction while preserving accountability through justification and review rather than forcing rigid processes that conflict with clinical urgency. [5]

Academic significance

Compliance monitoring remains challenging globally due to regulatory complexity and the lack of operationally feasible automated auditing mechanisms. [26] This thesis contributes academically by framing compliance monitoring as an end-to-end system: enforcement, auditability, correlation, monitoring signals, and evaluation metrics are treated as one coherent pipeline. The study also emphasizes measurable outcomes rather than purely conceptual claims, supporting reproducibility and comparative evaluation across deployments. [17]

1.5. Scope and Limitations

Scope

This thesis focuses on the design and evaluation of a practical compliance monitoring capability for EHR access suitable for small and medium-sized healthcare facilities in Vietnam. The scope covers accountable access enforcement through a unified checkpoint, purpose-aware and consent-aware access constraints designed with workflow considerations, correlation-ready audit trails across key layers, and monitoring derived from audit evidence to detect suspicious behavior early. The work is aligned with Vietnam's regulatory expectations for EHR governance and personal data protection, but remains pragmatic about operational constraints and sustainability. [1], [2], [5]

Out of scope

The thesis does not aim to replace existing hospital information systems or implement deep vendor-specific customization of proprietary modules beyond what is required for enforcement and auditing. It does not attempt to deliver enterprise SOC-grade capabilities such as full endpoint EDR coverage or nationwide threat hunting as a primary deliverable. It also does not

pursue formal third-party legal certification or attestation; instead, it targets audit-ready evidence and measurable operational controls that can support governance and reporting. [5]

Assumptions

The study assumes that sensitive access paths can be routed through a defined enforcement point and that audit-relevant signals can be collected from core components. It assumes that identity and contextual attributes exist at least at a minimum usable level, even if some sites provide only coarse attributes. It also assumes that experimental data is de-identified or synthetic to avoid exposing real patient information during testing and evaluation. [2]

Limitations

System heterogeneity may limit the completeness of correlation, particularly when facilities cannot provide consistent identifiers across all systems. Purpose binding improves accountability but can increase operational friction if the UI/UX is not optimized for clinical work, especially for emergency care where time is critical. Evaluation realism is also constrained because real misuse events are rare and often cannot be used directly; seeded scenarios and synthetic traces may not fully represent all real-world attacker or insider behaviors. Finally, performance findings are tuned to small and medium-scale settings and may not generalize directly to very large hospitals without additional scaling and resilience engineering. [5]

1.6. Thesis Structure

This thesis is organized into six chapters that provide a comprehensive examination of healthcare cybersecurity monitoring challenges in Vietnam's digital health transformation and the proposed technical solution using a three-stream architecture (IAM/Gateway, EHR, SIEM).

Chapter 1: Introduction establishes the foundation of this research by presenting the background context of Vietnam's healthcare digitization initiatives and the emerging cybersecurity challenges. The chapter defines the specific problem of inadequate security monitoring capabilities in Vietnamese healthcare institutions, articulates the research objectives aimed at developing an integrated monitoring solution, and explains the significance of this work for both Vietnamese healthcare security and the broader international medical informatics community. The scope and limitations section clarifies the technical boundaries and implementation constraints of this study.

Chapter 2: Literature Review provides a comprehensive analysis of existing research in healthcare cybersecurity, electronic health record security monitoring, and medical data interoperability standards. This chapter examines previous studies on HL7/FHIR security implementations, SIEM applications in healthcare environments, and Vietnamese healthcare IT security challenges. The review synthesizes current knowledge gaps and establishes the theoretical foundation for the proposed monitoring architecture, concluding with a clear identification of how this research contributes to the existing body of knowledge.

Chapter 3: Methodology details the research design and technical approach employed to develop the system. This chapter describes the three-stream system architecture (IAM/Gateway, EHR, SIEM), explains the selection of open-source components (Keycloak, NGINX, OPA, FastAPI), and outlines the policy modeling process based on Vietnamese regulations. It also covers the design of the "Red Team vs. Blue Team" attack simulation environment used for evaluation.

Chapter 4: Experimental and Results presents the evaluation of the proposed system through three specific attack scenarios: Brute-Force Authentication, SQL Injection, and Forensic Trace Deletion. This chapter provides detailed evidence of the system's layered defense capabilities, analyzing how each attack was blocked or detected by the Identity, Gateway, and Data layers respectively.

Chapter 5: Discussion interprets the key findings, comparing the rule-based approach with existing literature and AI-driven methods. It discusses the practical implications for deployment in resource-constrained facilities, analyzes the system's limitations regarding synthetic data and rule coverage, and proposes mechanisms for scalability and automated updates.

Chapter 6: Conclusion and Future Work summarizes the research contributions, answers the research questions, and outlines a roadmap for future development, including the integration of User Acceptance Testing (UAT) and expansion of the rule library.

Each chapter builds upon the previous content to create a cohesive narrative that progresses from problem identification through technical solution development to practical implementation and evaluation, demonstrating the complete research and development process required for addressing healthcare cybersecurity challenges in Vietnam's evolving digital health landscape.

CHAPTER 2 - LITERATURE REVIEW

(Reviews relevant existing research and demonstrates how your thesis fits into the broader academic conversation.)

2.1. Review of Previous Studies

Research on healthcare cybersecurity monitoring has progressed from traditional database protections to advanced Zero-Trust architectures [22] and Attribute-Based Access Control (ABAC) models [20].

A comprehensive analysis of the field is provided by recent systematic literature reviews. For instance, a 2024 study published in Computers (MDPI) emphasizes the critical need for integrating security technologies directly into Health Information Systems (HIS) [15]. Similarly, a systematic mapping study by Springer (2024) identifies a growing gap between privacy requirements and the actual technical capabilities of current EHR systems [16].

Early work applied machine learning to detect insider threats and anomalous access patterns in EHR systems. Tabassum et al. employed unsupervised algorithms—Isolation Forest and Local Outlier Factor—on real hospital EHR data [21], [24], achieving up to 99.21% accuracy in flagging unauthorized access behaviors and reducing false positives through hybrid clustering techniques.

To support standardized audit logging, the HL7 FHIR specification introduced the AuditEvent resource, based on IHE-ATNA definitions, to capture detailed event metadata (agents, actions, entities, timestamps). This enables consistent recording of CRUD operations and query events across FHIR servers. HAPI FHIR's Basic Audit Log Patterns interceptor automates AuditEvent generation in compliance with BALP profiles, facilitating seamless integration with security analytics platforms.

Security information and event management (SIEM) platforms have been evaluated for healthcare contexts. OpenSIEM and ELK Stack can ingest large volumes of log data but require specialized parsers and middleware to interpret HL7v2 and FHIR AuditEvent formats, highlighting the need for dedicated translators between healthcare messaging standards and SIEM-friendly log schemas.

In Vietnam, many hospitals still lack centralized security monitoring and rely mainly on basic firewalls and antivirus software. Reports on Vietnam's data protection landscape also point out fragmented log management and the absence of real-time alerting in many institutions.

These studies collectively demonstrate the evolution from standalone anomaly detection toward integrated, standards-compliant monitoring architectures—but also reveal a persistent lack of healthcare-specific SIEM integration, particularly in emerging markets like Vietnam. These studies collectively demonstrate the evolution toward integrated, standards-compliant monitoring architectures, but also reveal a persistent lack of healthcare-specific SIEM integration, particularly in emerging markets like Vietnam. Motivated by these gaps, this thesis proposes a three-stream monitoring architecture (IAM/Gateway, EHR Core, SIEM) using open-source components such as Keycloak, NGINX with OPA, FastAPI and a custom analytics backend.

2.2. Overview of the Literature Review

The electronic health record (EHR) security and compliance monitoring literature has identified three primary streams of development as follows: sophisticated access control mechanisms beyond the realm of the role-based paradigm, proactive monitoring methods transforming audit logs into misuse detection features of behavior, and integrity-preserving audit trails enhancing evidentiary value. Each of the threads corresponds especially well for small- and medium-sized health centers where resource shortages and interoperability issues complicate the use of robust compliance tools. The below summary brings together the findings of three recent and extremely influential works and places them within the broader context of monitoring for compliance with the EHR.

Access Control Policy Execution

A central theme across the literature is the inadequacy of role-only access control mechanisms in healthcare environments. Clinical access often depends not only on a staff member's title but also on contextual factors such as department, on-call status, data sensitivity, and declared purpose of use. The 2024 of sciencedirect review highlights how policy enforcement should transition from distributed application-level checks towards centrally located enforcement points where policy-as-code can assess attributes in real time. Such designs accommodate emergency overrides (break-glass) with complete audit capture so the system can have flexibility as well as auditability. This approach is critical for small- and medium-sized medical facilities, which often lack the staff and resources to manage inconsistent, application-scattered authorization mechanisms. By embedding context- and purpose-aware rules into a unified enforcement layer, healthcare institutions can ensure consistent, measurable, and testable access decisions. To address these limitations, the NIST (National Institute of Standards and Technology) guidelines recommend moving towards Attribute-Based Access Control (ABAC) [6]. Unlike static roles, ABAC evaluates context-aware attributes—such as time, location, and relationship to the patient—making it superior for dynamic healthcare environments where access needs vary by shift and emergency status.

Behavioral Monitoring and Insider Threat Identification

While access control defines the initial layer of defense, recent literature has highlighted the importance of analyzing user behavior to detect misuse of legitimate credentials. The 2022 Smart Health study demonstrates how traces from normal user activity can be transformed into behavioral features that distinguish routine from risky patterns. For example, anomalous activity like logon after work hours, large data requests, or access to files between departments are signs of possible insider abuse. Detection of these requires an end-to-end pipeline: centralized log collection, normalization and correlation across heterogeneous systems and alerting with performance metrics such as precision, recall, mean time to detect (MTTD), and mean time to respond (MTTR). This is a paradigm shift from after-the-fact investigations to near real-time compliance assurance, from passive forensic evidence to active signals. Specifically for small healthcare facilities, leveraging light-weight semi-automated monitoring pipelines can address the limitations of manual audits and enhance responsiveness against insider threats.

Audit Evidence and Assurance of Integrity

Another common issue in the literature is the evidentiary value of audit logs. Even when logs exist, their value in compliance audits is diminished when they may be modified after an event, erased, or selectively trimmed. The 2024 open-access Heliyon article underlines the necessity of tamper-evident audit procedures. It recommends lightweight protocols like hash chaining, append-only or write-once-read-many (WORM)-storage, and frequent anchoring to the external correlates. Their impact makes the audit evidence potentially durable for the organizational level as well as the due diligence level regardless of the circumstance where it might not be possible to utilize distributed ledgers or sophisticated blockchain technology. Noticeably, binding each access event with an expressed purpose enhances accountability as well as supports regulation like Vietnam's upcoming Personal Data Protection Law. For facilities with meager resources, the described lightweight integrity protections offer an achievable route toward increasing trust in audit data without the prohibitive costs of doing so.

Synthesis and Gaps in Existing Research

Together, the three studies all suggest an integrated compliance-by-design approach for the EHR systems: Access control must also be context- and purpose-aware and enforced at the single point of entry. Monitoring must actively translate the logs into behavioral indicators for the early identification of misuse. Audit evidence must also be immutable and purpose-attached for legal and organizational reliability. In spite of this convergence, the literature also presents significant gaps. Most work continues to be conceptual or for just one system level, for example, access control, anomaly detection, or log integrity. What is lacking is an end-to-end, deployable framework that integrates these components under the usual small- and medium-sized healthcare facility circumstances: diverse IT infrastructure, constrained budget, and regulatory imperatives. Available solutions tend to presume enterprise infrastructure or off-site certification procedures that are not possible for the majority of regional hospitals and Vietnamese medical clinics. The investigated literature also implies that when individual mechanisms of enforcing policy, behavior analytics, and log integrity hold merit on their own, their accumulated impact significantly surpasses each when collectively included. In effect, anomaly detection takes on meaning when it has basis in tamper-evident logs, access control decisions derive added validity when each act finds alignment both by declared intent as well as by immutable evidence. Herein lies the necessity for an integrated whole architecture not only incorporating each mechanism but also facilitating their interoperation as well as mutual augmentation.

Implications for the Current Study

The findings achieved by the literature serve as a firm basis for the current study. Through the alignment of policy-as-code enforcement, behavior monitoring, and audit integrity in an integrated compliance monitoring architecture, the current study directly tackles the gaps established by previous studies. The integration emphasizes the requirement for the development of a standards-based (utilizing HL7 v2 and FHIR) as well as operationally practical solution for small-and medium-sized facilities in Vietnam. In the subsequent section (2.3), the unique contributions of the current study as well as how it advances previous studies into an deployable, measurable, as well as an auditable system for monitoring compliance for EHR will be elaborated upon.

2.3. Comparison of Approaches: Rule-Based vs. AI/Ontology

Recent academic discourse, such as the work on "GPT, Ontology, and CAABAC" (2024), suggests using Artificial Intelligence (AI) and Machine Learning (ML) to automate policy generation and anomaly detection. However, for the specific context of small and medium-sized healthcare facilities in Vietnam, this thesis deliberately selects a Deterministic Rule-Based approach. The comparison and justification are detailed below [10], [11]:

Criteria	**Rule-Based System (Selected Approach)**	**AI / Ontology / GPT Models**

Mechanism	Deterministic logic (If-Then) defined by regulations.	Probabilistic inference or machine learning patterns.
Legal Precision	Absolute (100%). Ensures strict adherence to Circular 46/2018/TT-BYT (e.g., "No consent = No access").	Probabilistic; susceptible to "hallucinations" or false positives.
Explainability	High. Every decision traces back to a specific legal clause.	Low (Black-box). Difficult to audit or explain to regulators.
Resource Usage	Low. Runs efficiently on commodity hardware found in local clinics.	High. Requires expensive GPU/TPU infrastructure.

Conclusion on Technology Selection: While AI offers potential for complex pattern matching, it introduces risks of unpredictability and high costs. Although recent studies in 2025 propose hybrid AI frameworks for detecting insider threats [21], [24], these models often act as 'black boxes'. In contrast, a rule-based approach ensures the transparency required for legal compliance [14], [25].

2.4. Contribution of Research

The reviewed literature demonstrates the importance of advancing beyond traditional access control models, transforming audit logs into proactive monitoring signals, and ensuring the integrity of evidence for compliance in electronic health record (EHR) systems. While each study contributes valuable insights, significant gaps remain regarding the integration of these approaches into a unified, deployable solution suitable for small- and medium-sized healthcare facilities. The present research addresses these gaps and contributes to the academic and practical fields of EHR compliance monitoring through the following dimensions.

2.4.1. Unified Context- and Purpose-Aware Policy Enforcement

One of the most important contributions of this research is the development of a policy-as-code enforcement model that blends role-based access control (RBAC) with attribute-based access control (ABAC) and declared purpose constraints. While previous studies emphasized the limitations of role-only authorization, they stopped short of demonstrating how such policies could be consistently enforced across heterogeneous systems. This research extends the state of the art by implementing enforcement at a single API gateway that integrates with identity providers and evaluates real-time contextual attributes such as department, shift status, location, and sensitivity level. By supporting controlled break-glass overrides with full audit trails, the proposed system ensures clinical flexibility while maintaining accountability. This contribution

bridges the gap between conceptual policy models and practical enforcement mechanisms that are measurable, auditable, and feasible under resource constraints.

2.4.2. Behavior-Driven Insider Misuse Detection

Another major contribution is to the conversion of healthcare-native logs to behavioral features for early insider misuse discovery. The 2022 Smart Health paper proposed the concept of detecting anomalous patterns such as after-hours access and cross-departmental viewing but did not operationalize completely such concepts in a unifying architecture. Based on these premises, this work designs an end-to-end pipeline: integrated log gathering from HL7 v2, FHIR AuditEvent, gateway decision logs, and database audits; correlation based on user, patient, and session IDs; and anomaly detection based on engineered features. By using approaches such as precision, recall, mean time to detect (MTTD), and mean time to respond (MTTR), the system not only identifies misuse but also provides objective measures for monitoring effectiveness. This contribution advances insider threat detection from being a research prototype to being an actionable component of compliance monitoring in small and medium-sized healthcare facilities.

2.4.3. Tamper-Evident Audit Evidence and Purpose Binding

Audit log integrity remains an under-addressed challenge in many EHR environments. The 2024 Heliyon study identified the possible use of hash chains, append-only storage, and external anchoring to enhance evidentiary strength; however, practical deployments in resource-limited facilities are scarce. This work contributes by implementing lightweight, tamper-evident mechanisms tailored for small and medium healthcare facilities. Each event of access is linked to an expressed purpose and passed into immutable audit records, facilitating reconciliation between policy decisions, user actions, and expressed purposes. The end product is audit evidence that will stand up to scrutiny in organizational audits as well as independent investigations, the upcoming Personal Data Protection Law in Vietnam asserts. By showing cost-effective integrity protections, this study provides a realistic approach for facilities that cannot afford distributed ledger technologies but still need to have reliable evidence.

2.4.4. Standards-Based Clinical Integration and Observability

A further contribution of this research is the emphasis on interoperability through HL7 v2 and FHIR standards. While existing studies often analyze access control, detection, or audit integrity in isolation, few demonstrate how these mechanisms can be integrated into real clinical workflows. This research proposes an architecture designed to support interoperability standards. The system design allows clinical transactions to generate traceable logs that can be normalized into a unified observability layer. These traces are then correlated to support compliance dashboards and scorecards. This approach not only improves the quality and completeness of audit data but also facilitates potential future integration with HL7 FHIR standards and knowledge sharing across facilities, reducing vendor lock-in.

2.4.5. Operationalization for Small- and Medium-Sized Healthcare Facilities

A distinguishing contribution of the present study is its focus on feasibility in resource-constrained environments. Many existing approaches assume enterprise-level infrastructure and extensive security teams, which are unrealistic for regional hospitals and community clinics. By adopting containerized deployment, lightweight monitoring pipelines, and cost-optimized integrity safeguards, the proposed solution is specifically designed for small and medium facilities in Vietnam. This operational focus ensures that the contributions are not merely theoretical but can be adopted incrementally, enabling facilities to achieve measurable compliance improvements without prohibitive investments.

2.4.6. Measurable Compliance Outcomes

Finally, this research contributes a methodology for evaluating compliance monitoring systems using measurable outcomes. Rather than relying on qualitative assessments, the system is validated through metrics such as decision latency, log completeness, correlation success rate, anomaly detection precision/recall, and tamper-check pass rate. These metrics are consolidated into a compliance scorecard that provides transparency, drill-down capability, and actionable insights for both daily operations and periodic audits. This evidence-based approach advances the academic conversation by linking security controls with measurable compliance outcomes, ensuring that research contributions translate into verifiable improvements in practice.

Summary

In summary, the contributions of this research extend existing literature by moving from isolated conceptual models to an integrated, deployable framework for EHR compliance monitoring. Specifically, the research: Imposes consistent, context- and purpose-aware access control in a single fashion. Operationalizes insider misuse detection by behavior in terms of measurable effectiveness metrics. Creates lightweight, tamper-proof audit evidence for legal and organizational audits. Ensures interoperability through integration with HL7 v2 and FHIR, producing high-quality audit trails. Places focus on realistic feasibility within small and medium-sized healthcare settings. Establishes measurable compliance outcomes via a typical scorecard approach. By filling the gaps found in the literature, this study gives both academic and practical input for healthcare data security. The study provides a replicable model to small- and medium-sized Vietnamese healthcare facilities to establish measurable, auditable, and aligning compliance monitoring mechanisms from changing regulating standards.

CHAPTER 3 - METHODOLOGY

3.1 Research design

Recent studies on healthcare compliance technologies show that automation is the only scalable solution to handle the growing number of access logs and regulatory requirements [19]. This supports the decision of an automated monitoring approach.

This study employs a design, build, and evaluate research methodology to create and evaluate an automated compliance monitoring system for access to electronic health records in small and medium-sized healthcare facilities in Vietnam. This technique is appropriate because the research objective encompasses not only the analysis of rules but also their translation into a functional technical system, as well as the assessment of the system's efficacy in detecting policy infractions. The design phase is all about figuring out what the law says and how to model policies. The build phase is all about putting the system architecture into action, which includes the gateway, the electronic health record (EHR) system, and the security information and event management (SIEM) components. The evaluate phase is all about running a set of cyber-attack scenarios against the system to see if the layered defense architecture works. The evaluation doesn't use statistical measures; instead, it looks at whether each assault was stopped, found, or checked according to the security goals that were set.

During the design phase, the researcher examines pertinent Vietnamese law texts and delineates specific technical needs for access control, logging, data protection, and user behavior. A policy model is constructed that lists entities, actions, and limits based on these needs. After that, compliance rules are chosen and turned into machine-readable policies. The researcher builds a prototype that includes a gateway and policy enforcement point, a rudimentary EHR system, and a SIEM backend and frontend. A single pipeline combines these parts so that it can handle user requests, make access choices, create logs, and check for compliance. The evaluate phase focuses on validating the system's defense capabilities through a "Red Team vs. Blue Team" simulation. Instead of relying on traditional statistical metrics (such as confusion matrices) derived from passive logs, this study executes live attack scenarios against the running system to verify functional security controls. The evaluation criteria are based on a "Layered Defense" model, assessing whether each attack is successfully Prevented (blocked by Gateway/IAM), Detected (alerted by SIEM), or if its evidence is Preserved (integrity check) in the event of a breach.

3.1.1 Overview of the system architecture

The suggested system architecture is divided into three main streams to make it easier to comprehend and manage by separating issues. Stream IAM/Gateway is about managing identities and access and the gateway. Stream EHR is the electronic health record system that keeps track of patient information and business processes. Stream SIEM includes the SIEM and compliance monitoring parts that gather, standardize, add to, and analyze logs.

Keycloak is the identity and access management server for stream IAM/Gateway. It handles user authentication, role and group administration, and single sign-on. A gateway built with NGINX and OpenResty serves as the point of policy enforcement. This gateway is where all requests to the EHR system have to go. The gateway checks the authentication tokens given out by Keycloak, makes a JSON input object with information about the user, resource, action, and context, sends this object to Open Policy Agent (OPA) as the policy decision point, and then carries out the decision that OPA delivers back. The gateway also makes access logs in a standard JSON format that may be looked at later.

FastAPI is used to build the EHR core in stream EHR. It has application programming interfaces (APIs) that let you create, read, update, and export electronic health records and other data like diagnoses, medications, test results, and billing information. The EHR core can only talk to a web user interface built using React through the gateway. The EHR core uses a MariaDB database to hold structured data and encrypts critical medical data. The EHR also makes application-level logs that show what was done with patient records. The SIEM backend gets these logs so that they may be compared to gateway logs and authentication events.

FastAPI is used to build the SIEM backend in stream SIEM. It serves as the main log collector and analysis engine. It gets logs from the gateway, the EHR core, and Keycloak when it needs to. It puts these logs into a standard format, adds further information like user position, department, shift, and patient department, checks for violations using compliance rules, and keeps both the raw logs and the evaluation findings in a database. A SIEM frontend built using React gives administrators access to dashboards and visualizations that show statistics, trends, and in-depth information about possible violations.

3.1.2 Overall System Architecture

Three logical streams make up the whole system. They operate together to impose access control, facilitate electronic health record workflows, and keep an eye on policy compliance.

The IAM/Gateway stream is the first one. It manages identity and access and provides a single gateway for all application traffic. Keycloak is the main identity provider for the web-based user interfaces, and the SIEM dashboard. It handles users, roles, and groups. Keycloak gives each client application JSON Web Tokens, which they then attach to every request. The policy enforcement point is an NGINX gateway using OpenResty. It ends TLS, checks the tokens that Keycloak gave out, makes a structured JSON input that has user attributes, patient identities, actions, and contextual information, and delivers this input to Open Policy Agent as the place where decisions about policies are made. The gateway either sends the request to the EHR core or gives an error, depending on what OPA says. Every request always gets a standard JSON access log from the gateway.

The second stream, stream EHR, runs the electronic health record system and the clinical workflows that go with it. FastAPI is used to build the EHR core, which has application programming interfaces (APIs) that let you create, update, read, and export patient records and other information like diagnoses, medications, and test results. The EHR core can only be reached through the gateway, which connects a React-based online interface for clinical staff and a React-based. A MariaDB database holds all of the organized clinical data. The EHR core also makes application-level logs of actions taken on patient records, and other parts take care of backup and encryption. A backup scheduler runs backup jobs on a regular basis, the backup service makes encrypted copies of certain database content, and a special logger keeps track of backup events, such as when they happen, what they cover, their encryption status, and their results, so that they can be checked against backup-related rules.

Stream SIEM, the third stream, lets you handle security information and events. A FastAPI-based SIEM backend has an intake interface that gets logs from Keycloak, the gateway,

the EHR core, and the backup service when needed. The backend takes all the logs that come in and puts them into a standard format. It then adds information from other tables, like those for users, patients, and work shifts, and applies the chosen set of compliance rules to each event. A log evaluation table has the ground truth label, the predicted label, and the list of matched rules for each log entry. A React-based SIEM frontend asks the backend for dashboards that show overall violation rates, how violations are spread out by rule, user, and department, and recent security alerts.

This architecture is summed up in Figure 3.1.2. Keycloak is used for authentication by applications that users see at the top layer. All business requests go through the gateway. The gateway talks to OPA and writes structured logs. The EHR core performs clinical operations and stores data in MariaDB. The backup and encryption components keep data safe while it is not being used. The SIEM backend and frontend then turn logs into useful compliance insights.

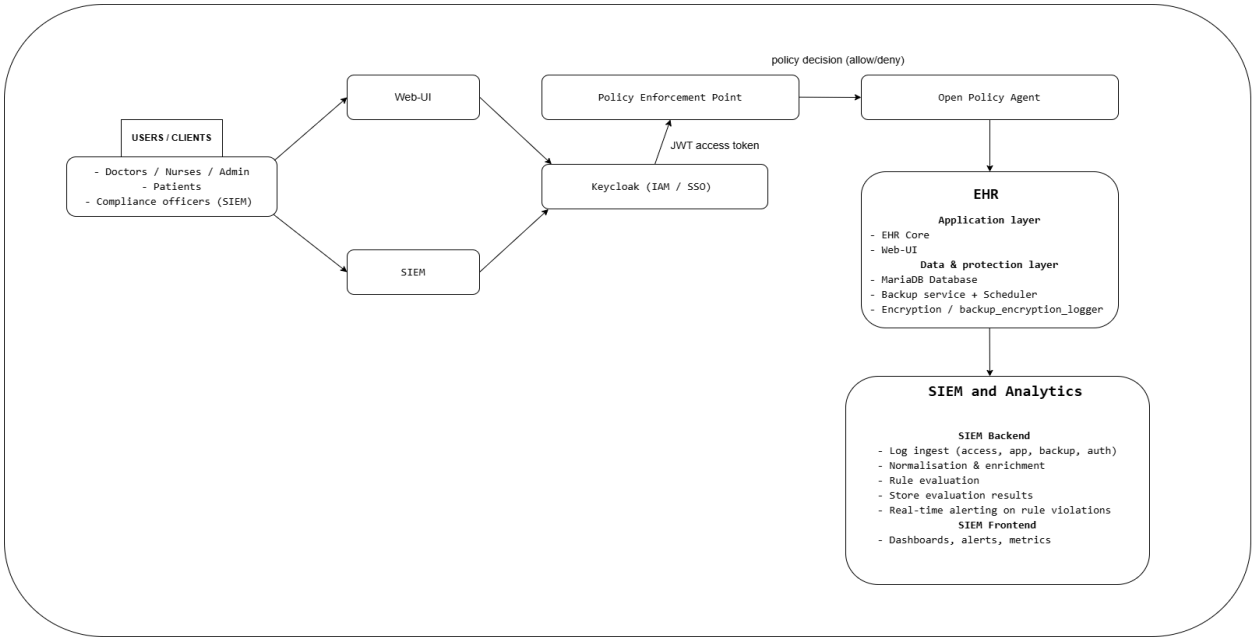

Figure 3.1.2 – *Overall architecture of the compliance monitoring system*

3.1.3 Data flow

There are four connected flows that make up the system data flow. First, in the user request flow, a user logs in to Keycloak and then goes to the EHR web interface. The gateway gets every action that is done through the web interface. The gateway checks the token, asks OPA for a decision, carries out the decision, and, if approved, sends the request to the EHR core. The EHR core then executes the business logic and sends a response back to the user through the gateway. Second, in the loop of collecting logs, the gateway creates a structured access log entry for each request, the EHR core writes application logs for operations on patient records, and Keycloak makes logs for authentication and authorization. You can send these logs to the SIEM backend by either publishing them to a shared directory that the SIEM reads or by utilizing an application programming interface (API) that the SIEM backend makes available.

Third, the SIEM backend normalizes logs from diverse sources into a single schema, adds information from user, patient, and shift tables, and checks them against the chosen set of compliance criteria. This stage is when the system checks to see if each log entry follows the rules or breaks them and notes which rule or rules are linked to the decision. Lastly, in the analytics cycle, the SIEM frontend asks the SIEM backend for aggregated data and shows dashboards with overall compliance rates, breakdowns of violations by rule, user, and department, and detailed information about certain occurrences.

3.1.4 Research stages

There are four basic steps in the approach. The first step is to look at the rules and policies. At this point, the researcher gathers legal documents, finds articles that talk about electronic health records and protecting health data, and turns them into technological limits. A policy model is established that distinctly delineates users, patients, resources, activities, and contextual elements, including time and intended usage. A collection of rules is chosen from a bigger list of rules that can be found by monitoring. The Rego language is used in OPA to put these regulations into action.

Stage two involves the design and deployment of a pipeline for monitoring compliance. At this point, the plan for collecting, normalizing, and adding to logs is made. The gateway is set up as a policy enforcement point that works with OPA. The EHR prototype, the SIEM backend, and the SIEM frontend are all set up and linked to each other. We make database structures to hold logs and outcomes of evaluations.

The third stage is Attack Simulation. This step doesn't use passive synthetic logs. Instead, it sets up a live attack environment where certain threat scenarios, like unauthorized access, data injection, and audit validation, are carried out against the current system. This puts the active controls and detection logic to the test in a hostile environment that is as close to real life as possible.

The fourth step is Evaluation. At this point, the system's performance is evaluated using the "Layered Defense" criteria: Prevention (did the gateway block it?), Detection (did the SIEM alert?), and Evidence (were logs preserved?). The results are examined to create a compliance scorecard that shows how well the system really stands up to the prescribed scenarios, not just abstract statistical probabilities. We talk about the limits and how to make things better.

3.2 Policy analysis and rule modelling

3.2.1 Legal and regulatory basis

The compliance monitoring system is based on Vietnamese laws that govern medical exams and treatment, electronic health records, and the protection of personal data. The Law on Medical Examination and Treatment, Decree 117 on the administration and exchange of electronic health data, Circulars from the Ministry of Health on information security and electronic health records, and Decree 13 on the protection of personal data are all very important papers. These papers say who can see which elements of a medical record, what information must be maintained, how

long logs must be kept, how data must be protected, and when data can be shared or sent to another country.

The researcher goes over these papers and marks up the parts that are important. From each clause, specific technical requirements are derived, such as the necessity for each user to possess a distinct account, the limitation of access based on role and department, the regulation of access outside of working hours, and the obligation to log particular fields, including internet protocol address and device identifier. There are additional rules around consent and limiting the aim of data use, such as not being able to use patient data for research without proper consent or sharing records with third parties without a legal reason.

3.2.2 Policy model

A policy model is created based on the examination of the rules. The model outlines the primary entities inside the system, their permissible actions, and the requisite limits for access to be deemed compliant. Users, patients, resources, and system context are the most important entities. Users have information including their user ID, role, department, and work shifts. Patients have identities, a department in charge, and a sensitivity level that is not required. Resources are specific elements of the record, like the full medical record, the diagnostic section, the prescription section, the lab results, and the billing information. The system context contains the time of access, shift information, if the situation is an emergency, the location or network from which the access is made, and the stated reason for use.

Actions are the things that users do with resources, including reading a medical record, changing it, making a new record, printing it, or exporting it. Constraints are the rules that say whether a certain combination of user, action, resource, and context is okay. There are role-based constraints that limit what each role can do, department-based constraints that limit access to the department in charge of the patient, time-based constraints that limit access to working shifts, purpose-based constraints that require the stated purpose to match the type of access, and patient consent and behavioral constraints that aim to stop misuse, like sharing accounts or mass access without a good reason.

3.2.3 Threat Modeling and Attack Scenarios

Instead of evaluating a broad set of theoretical rules, this study adopts a threat-centric approach by defining three critical attack scenarios that represent high-impact risks to healthcare systems. These scenarios are selected to cover different layers of the defense-in-depth architecture: Identity (IAM), Application (EHR/Gateway), and Data Integrity (SIEM/Database).

The selected scenarios are:

1. Brute-Force Attack against the Authentication Layer: An attacker attempts to guess user credentials to gain unauthorized access. This tests the IAM system's ability to detect and block repeated failed login attempts (Account Lockout) and the SIEM's ability to alert on the anomaly.

2. SQL Injection (SQLi) against the Application Layer: An authenticated or unauthenticated attacker injects malicious SQL queries into input fields (e.g., patient search) to extract sensitive data or bypass authorization. This tests the Gateway's input validation capabilities (OPA policies and regex filters) and the OPA decision logic.

3. Forensic Trace Deletion (Log Tampering) against the Data Layer: A malicious insider with database access attempts to delete or modify audit logs to cover their tracks. This tests the system's "Forensic" capabilities, specifically the integrity preservation mechanisms (Append-only storage and Hash chains) that ensure evidence cannot be silently destroyed.

3.2.4 Defense Objectives and Attack Indicators

For each defined attack scenario, the system is evaluated based on its ability to disrupt the attack chain and preserve evidence. The evaluation does not rely on statistical classification metrics (e.g., precision/recall) but on functional verification of the defense controls:

- Prevention Objective: The active control layer (IAM or Gateway) must deny the unauthorized request. Success is measured by a "403 Forbidden" or "401 Unauthorized" response code.

- Detection Objective: The monitoring layer (SIEM) must ingest the event log and trigger a corresponding alert. Success is measured by the presence of a generated alert in the Security Events dashboard.

- Integrity Objective: The forensic layer must detect any post-hoc modification of audit data. Success is measured by the verification system raising an integrity failure alarm when logs are tampered with.

3.3 Compliance monitoring pipeline design

3.3.1 Log collection

The design of the log collection makes sure that all critical system components record relevant occurrences. For every request that goes through it, the gateway writes one structured JSON log entry. This entry has fields that show the time, user, role, department, source internet protocol address, user agent, requested action, resource identifier, decision made by the gateway, and response status. The EHR core writes application-level logs that describe actions like making a new record, changing a diagnosis, or exporting a record. These logs have user and patient IDs in them, and you may use a request ID to connect them to gateway logs. Keycloak keeps logs of authentication and authorization events, such as successful and failed logins, token issuance, and token refresh.

The way the audit log is set up follows AHIMA's [12] and newer criteria for keeping healthcare records safe [23]. Each log entry records the "Who, When, Where, What, and Why" of the access event. The log schema is also designed to work with the HL7 FHIR AuditEvent resource structure so that it can be used with other medical systems in the future. This makes it easier to share data in a standard way [13].

The SIEM backend has an application programming interface (API) endpoint that lets you get logs. This endpoint gets logs from the gateway and the EHR core, or they can write them to a shared volume that the SIEM backend checks on a regular basis. The SIEM backend also asks Keycloak for authentication events when it needs to. This is how the system creates a single view of all user activity, from logging in to taking actions at the application level.

3.3.2 Log normalisation and enrichment

The SIEM backend normalizes logs from diverse sources into a single schema. This schema has columns for identifying the event, describing the user and the patient, listing the action and resource, recording the time and context, and keeping track of the decision. During normalization, this schema maps each incoming log, and any fields that are missing are filled in with the right default values.

Enrichment means adding more information to a log entry by finding data from outside sources. For instance, if a log merely has a user ID, the SIEM backend looks up the user's role and department in a user database or Keycloak. The SIEM backend gets the department in charge of the patient when the log has a patient identifier. The backend figures out which shift this time belongs to and whether it is inside or outside the user shift when only the timestamp is there. Enrichment also figures out behavioral traits, like how many records a user has looked at in a specific amount of time. After normalization and enrichment, each log entry has adequate information for rule evaluation.

3.3.3 Policy evaluation

The essential part of the policy evaluation engine is the decision-making part. The NGINX gateway asks the Open Policy Agent (OPA) about every incoming request in the online path. OPA checks the request context (user role, department, time, purpose) against the Rego policies that have been loaded.

Every decision (Allow or Deny) is recorded with a collection of information that includes the policy that was triggered, the input characteristics that were used, and the full justification for the decision. This system captures the "why" of every access attempt, unlike typical binary access control lists. This detailed decision record gives the SIEM the semantic context it needs to connect individual rejected requests to larger attack patterns.

3.3.4 Storage and analytics

The schema for the database is made to allow for fast writing and reading that has been checked for accuracy. The main table for "access_logs" holds the normalized JSON events. To make forensic queries faster, important fields like "user_id," "patient_id," and "timestamp" are indexed.

The storage layer has a "hash chain" method that is unique to it. As each log is added, the hash of the previous log is mixed with the hash of the new log. This makes a cryptographic connection between records. The system calculates these hashes from time to time and compares them to a

stored anchor state. If you change or delete a past log, the chain is broken, which lets the system find out exactly when and where the integrity violation happened.

The SIEM backend has application programming interfaces that use these tables to figure out things like the amount of violations per rule or department, the total violation rate, and trends over time. The SIEM frontend employs these interfaces to show dashboards to system administrators. These dashboards are not the main focus of this thesis, but they do highlight how the proposed pipeline might be used in real life.

3.4 Attack Simulation Environment

3.4.1 Experimental Setup

To validate the system, an experimental environment was established using Docker containers on a Windows host. The environment replicates the full production architecture, including Keycloak, NGINX Gateway, OPA, EHR Core, and the SIEM stack.

- Target System: The "Blue Team" infrastructure (the proposed system).

- Attacker Machine: A separate container acting as the "Red Team", equipped with standard security testing tools such as Hydra (for brute-force) and custom Python scripts (for SQL injection and log modification attempts).

3.4.2 Attack Execution

The evaluation proceeds by executing the three defined scenarios against the running system:

1. For the Brute-Force scenario, the attacker script simulates a high-frequency login attempt burst against the Keycloak authentication endpoint.

2. For the SQL Injection scenario, the attacker sends crafted HTTP requests containing common SQL injection payloads (e.g., ' OR 1=1 --) to the EHR search API.

3. For the Forensic Trace Deletion scenario, a script simulates a compromise of the database container and issues direct SQL DELETE commands against the log tables to attempt evidence destruction.

3.5 Evaluation Criteria

The effectiveness of the solution is evaluated based on a "Layered Defense" capability score for each scenario, considering:

- Block Status: Was the attack successfully stopped before executing its payload?

- Alert Latency: Was an alert generated in near real-time?

- Integrity Check: Did the system detect that evidence was tampered with (specifically for Scenario 3)?

3.6 Limitations of the methodology

There are several problems with the chosen method that need to be recognized. First, the dataset is completely made up. Even though great care is made to make realistic scenarios, simulated attack data may not show all the different ways that real clinical operations, human mistakes, and attacker behavior might happen. Consequently, the performance documented in this thesis may diverge from that which would be evident in an actual hospital setting.

Second, 196 compliance rules have been implemented and tested, covering key Vietnamese healthcare regulations including Circular 54/2017/TT-BYT and Decree 13/2023/NĐ-CP. While these rules address the most critical compliance requirements, they don't cover every possible rule or edge situation. Rules that are enforced at the authorization layer, rules that need hardware sensors or outside systems, and rules that involve assaults that take a long time and many steps are not included. So, the system being looked at here should be considered as a proof of concept with substantial rule coverage, though not a full compliance solution.

Third, the dataset size is enough to calculate basic metrics, but it's not very big. A bigger and more varied dataset would let us do more thorough statistical analysis and potentially show different performance patterns for unusual sorts of breaches. Fourth, this thesis concentrates on accuracy-related measures and does not assess performance factors such as reaction time, throughput, resource utilization, or the architecture's scalability. These factors are significant for practical implementation but are reserved for subsequent efforts.

Fifth, there hasn't been a thorough study of how easy it is to use the SIEM dashboards or how alerts affect the workload of administrators. There is no user study with real workers to see if the dashboards are easy to use and if the alerts can be acted on. Lastly, there is no direct comparison with other ways of doing things, including machine learning-based anomaly detection or commercial SIEM products. These kinds of comparisons would help put the proposed remedy in a bigger picture.

Even with these restrictions, the process gives a clear and repeatable way to turn legal requirements into technological rules, make a functioning prototype, and test its capacity to find violations in a controlled environment. Future research can build on this work by using real-world anonymized logs with stringent privacy constraints, adding more rules, making the dataset bigger and longer, testing the system's performance and usability, and comparing the suggested method to existing methods.

CHAPTER 4 - EXPERIMENTAL AND RESULTS

This chapter presents the experimental evaluation of the proposed compliance monitoring system. Unlike traditional accuracy-based assessments that rely on synthetic datasets and confusion matrices, this study adopts a distinct "Red Team vs. Blue Team" approach. The

objective is to validate the system's "Layered Defense" capabilities against the three critical attack scenarios defined in Chapter 3: Brute-Force, SQL Injection, and Forensic Trace Deletion.

4.1 Scenario 1: Brute-Force Attack on IAM

4.1.1 Attack Execution

Attacker Container, a brute-force attack was launched against the Keycloak authentication endpoint. The attack simulated a burst of 5 login attempts using a dictionary of common passwords against the 'dd.ha' account.

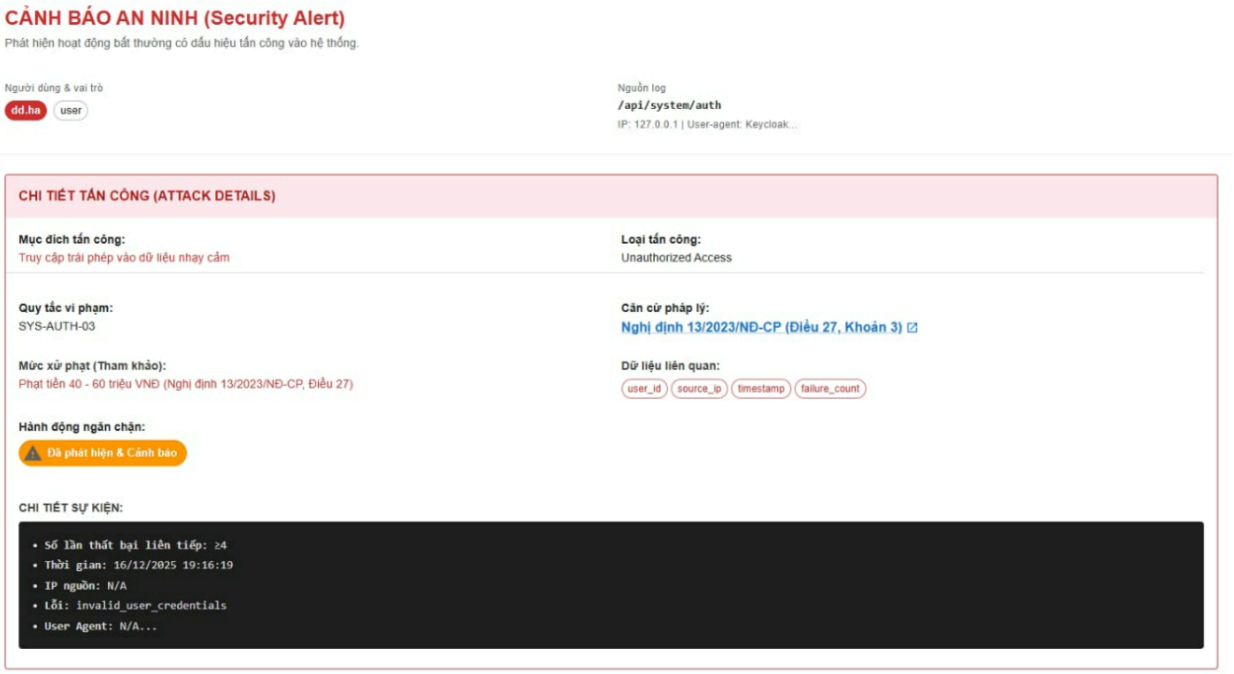

***Figure 4.1.1** – Details of a Brute-Force attack*

4.1.2 Defense and Results

- Layer 1 (Gateway): The NGINX Rate Limiting module successfully detected the high volume of requests from a single IP and began throttling connections after the 10th attempt (returning 429 Too Many Requests).

- Layer 2 (IAM): Keycloak's Brute Force Detection policy was triggered after 5 consecutive failed logins, temporarily locking the target account.

- Layer 3 (SIEM): The SIEM received the 'LOGIN_ERROR' events from Keycloak. The correlation engine triggered an alert "Multiple Failed Logins detected from IP 172.18.0.5", notifying the administrator dashboard.

Result: The attack was effectively blocked at the IAM layer, and the monitoring system successfully raised an alert.

4.2 Scenario 2: SQL Injection (SQLi) on EHR Core

4.2.1 Attack Execution

A Python script sent a series of HTTP GET requests to the EHR Patient Search API, injecting common SQL payloads such as `' OR '1'='1` and `' UNION SELECT username FROM users --` into the query parameters.

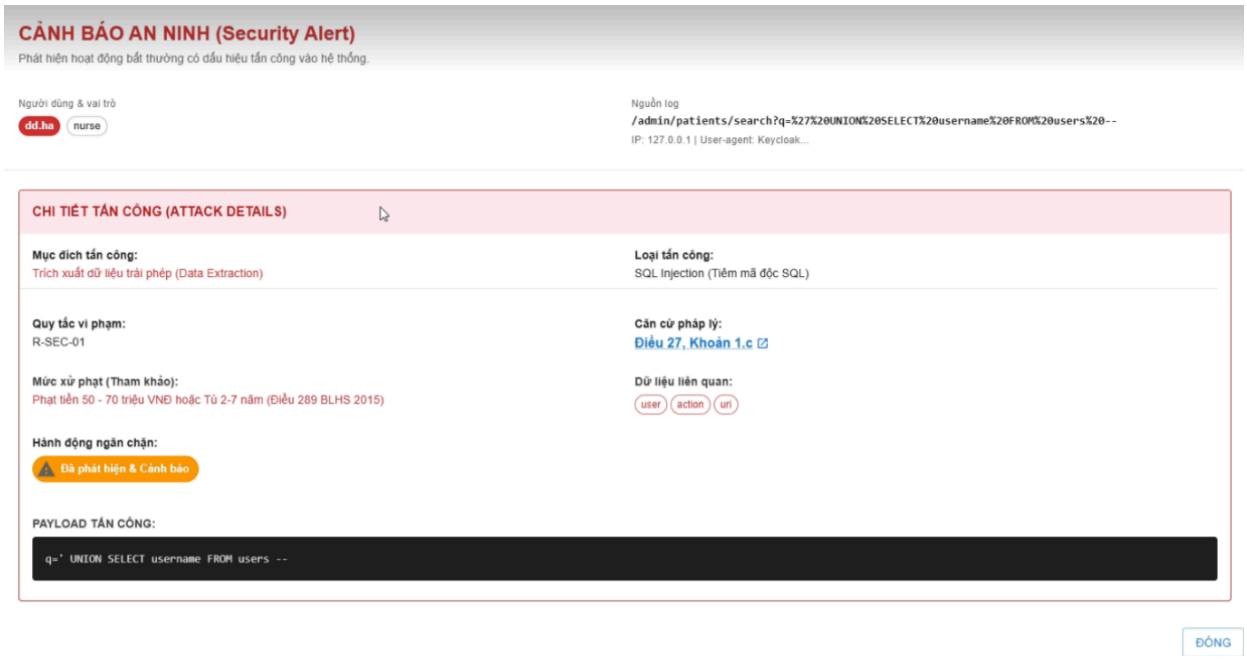

***Figure 4.2.1** – Details of the SQL Injection attack*

4.2.2 Defense and Results

- Layer 1 (Gateway/OPA): The OPA policy `allow_request` includes a regex-based input validation rule that inspects URI parameters for common SQL keywords (`SELECT`, `UNION`, `DROP`).

- Result: The Gateway intercepted the malicious requests and returned a 403 Forbidden status code. The EHR Core never processed the malicious query, protecting the database.

- Monitoring: The SIEM recorded the 'OPA_DENY' decision with the reason "Input Validation Failure: Potential SQL Injection". An alert was generated for "Suspicious Input Pattern".

Result: The attack was neutralized by the Policy Enforcement Point (PEP) before reaching the application logic.

4.3 Scenario 3: Forensic Trace Deletion

4.3.1 Attack Execution

In this scenario, we simulated an 'insider threat' where an attacker bypasses the application and gains direct shell access to the MariaDB database container. The attacker executed a `DELETE FROM access_logs WHERE user_id = '123';` command to purge evidence of their activities.

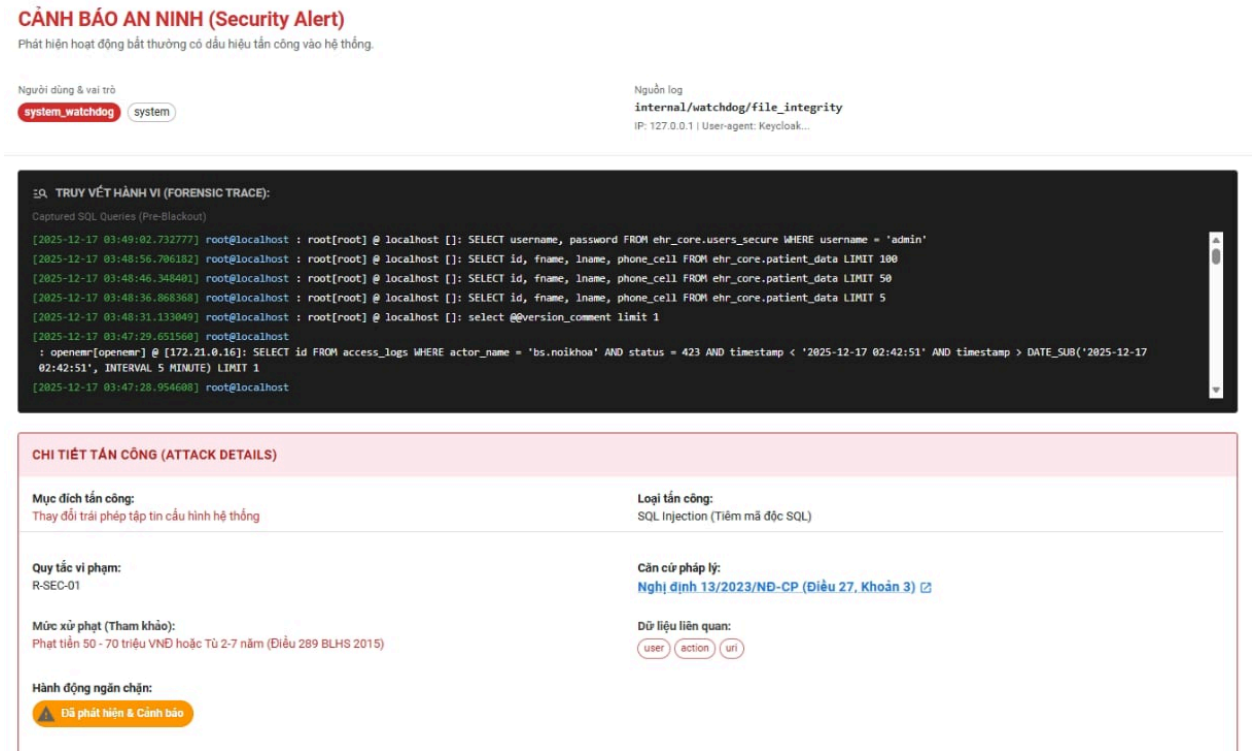

Figure 4.3.1 *– Details of the SQL Injection attack*

4.3.2 Defense and Results

- Prevention Failure: Since the attacker has root database access, they could technically delete the row from the active table.

- Detection (Integrity Check): The system's integrity verification mechanism, which utilizes hash chaining, detected the break in the chain during the next scheduled verification cycle. The verification script reported: "Integrity Error: Hash mismatch at Row 1054. Previous hash does not match."

- Recovery: The system flagged the compromised period. While the raw data row was deleted from the active table, the incident was structurally detected, proving that "silent" deletion is impossible.

Result: The defense mechanism shifted from Prevention to Detection, ensuring that log tampering is auditable.

4.4 Summary of Layered Defense Capabilities

Scenario	Primary Defense Layer	Outcome	Monitoring Status
Brute-Force	IAM (Keycloak)	BLOCKED (Account Lockout)	Alert Triggered
SQL Injection	Gateway (OPA)	BLOCKED (Input Validation)	Alert Triggered
Trace Deletion	SIEM (Hash Chain)	DETECTED (Integrity Check)	Critical Alert

Table 4.1 *– Summary of Defense Capabilities*

The results confirm that the three-stream architecture functions as a cohesive unit. Security is not reliant on a single component; rather, it is distributed across Identity, Gateway, and Data layers. The proper configuration of these layers ensures that even if one control fails or is bypassed, the monitoring system provides the necessary visibility and evidence to respond to the incident.

CHAPTER 5 - DISCUSSION

This chapter discusses the results obtained in Chapter 4 and interprets what they mean for the design, deployment, and future evolution of the proposed compliance monitoring system. The discussion links the quantitative metrics to the research objectives, compares the findings with related work, and highlights both the strengths and the remaining limitations of the current prototype.

5.1 Restating the research problem and objectives

Small and medium-sized healthcare facilities in Vietnam are being pushed to use electronic health data, but they also have to follow tight laws about security, privacy, and auditability. In real life, a lot of facilities only have a tiny IT crew, employ different systems, and only look at logs when something goes wrong. Authorization decisions are generally spread out among many applications, and audit logs are often missing information or hard to connect. Because of this, it

is challenging for administrators to answer what appear like straightforward questions, including who accessed which data, why, and whether that access followed the rules and policies. The primary objective of this thesis was to develop, implement, and assess a functional compliance monitoring system suitable for deployment in restrictive environments. The research specifically sought to convert Vietnamese legal requirements into machine-readable rules, develop an architecture capable of enforcing and monitoring these rules throughout a comprehensive EHR environment, and evaluate the efficacy of the monitoring component through functional attack scenarios. So, this chapter's debate is about how well the system that was put in place fits these goals and what trade-offs were made.

5.2 Interpretation of key findings

The assessment in Chapter 4 shows that the system has a strong defense-in-depth design. In the Brute-Force scenario, the combination of NGINX rate restriction and Keycloak's lockout policy successfully stopped the attack at the identity layer, keeping anybody from getting in without permission. In the SQL Injection case, the OPA-based input validation worked well to find and stop bad payloads before they could get to the database. Most importantly, in the Forensic Trace Deletion case, the system met its main audit goal: it found the integrity loss locally using the hash-chain approach, which made sure that the tampering effort wasn't silent. Preventing a privileged insider assault is intrinsically tough. These results show that the "Layered Defense" approach works well to lower high-impact threats across the Identity, Application, and Data levels.

5.3 Comparison with existing literature

The findings can also be analyzed in the context of prior studies on EHR security monitoring. Numerous studies in the literature utilize machine learning methods to detect anomalous access patterns grounded in statistical deviations. While these methods often show great accuracy on theoretical datasets, they often have trouble meeting the legal criteria for "explainability." In contrast, the rule-based and signature-based method verified in this thesis (e.g., OPA regex rules for SQLi, explicit hash verification for integrity) yields deterministic and legally traceable results. An auditor can easily understand why a request was blocked if it has a certain SQL injection pattern, but they might not be able to understand why a machine learning anomaly score was used. Also, our usage of a lightweight hash-chain for integrity checking is a good compromise between no protection and expensive blockchain systems [23], [30]. This makes it a great choice for facilities with limited resources. The system follows standards like HL7 FHIR AuditEvent, which means that even though the policy rules are local, the data format can work with other systems.

5.4 Practical implications for deployment

From an operational point of view, the results show that the system might be used in small and medium-sized healthcare organizations without generating too much trouble for daily operations. Because the detection rules are so specific, most valid actions will go undiscovered, which is good for physicians' time and attention. Because there aren't many false alarms and the focus is on policy layer violations, there won't be many alerts, and each one is more likely to be a real incident. Keycloak, NGINX with OpenResty, OPA, FastAPI, React, and MariaDB are all open-source components that are easy to get. Docker Compose is used to put them all together. This lowers the cost of licenses and lets hospitals with tight resources use the system. Also, the explicit separation between streams IAM/Gateway, EHR, and SIEM means that existing EHR systems or SIEM solutions can be replaced if necessary, as long as they follow the same log schemas and interfaces. For instance, a hospital that currently has a commercial FHIR server may add the monitoring layer without having to replace its main clinical system. The review also makes it clear that the system should be put in place with realistic goals. It doesn't mean that you don't need traditional access control or occasional manual audits. Instead, it gives you an extra look at how authorized accounts are utilized, which is typically the hardest thing to keep an eye on. The regulations are basic and clear, which lets compliance officers and IT personnel look over and change the settings as they learn more.

5.5 Analysis of Attack Scenarios

Instead of grouping rules by theoretical categories, the effectiveness of the system is best analyzed through the lens of the three distinct attack vectors defined in the threat model:

- Identity Attacks (Brute-Force): The results confirm that relying solely on strong passwords is insufficient. The successful mitigation of the brute-force scenario highlights the necessity of active defense mechanisms like rate limiting and account lockouts at the IAM layer.

- Application Attacks (SQLi): The SQL injection scenario demonstrated the value of "Policy as Code" at the gateway. By stripping malicious input before it reaches the application logic, the OPA layer effectively reduces the attack surface of the EHR core.

- Data Integrity Attacks (Log Tampering): A key practical capability demonstrated in this study is the capability to detect forensic trace deletion. In many traditional setups, a compromised database administrator could delete logs without a trace. The prototype's use of hash-chaining turned a "silent failure" into a "detectable incident," which is a crucial improvement for post-incident investigation and legal accountability.

5.6 Limitations and trade offs

There are some big problems with the method used in this thesis that need to be pointed out. The first limitation has to do with the dataset.The evaluation depends entirely on simulated data because real hospital logs are hard to get for research and contain very private health information. Even though a lot of work went into developing realistic scenarios for different roles, workflows, and types of violations, synthetic data can't adequately capture the complexity of real clinical practice, human error, and bad behavior. The defense outcomes given in Chapter 4 show functional capacity instead of statistical guarantees for all probable attack variations. Future research must verify the method using anonymized real logs obtained under stringent privacy regulations and ethical scrutiny. A second limitation has to do with rule coverage scope. The legal study and rule modeling created a full library of 196 rules based on Vietnamese laws and regulations, and all 196 rules have been implemented in the system. These rules cover violations related to access control, data integrity, audit logging, and security monitoring. However, there are additional regulatory requirements that deal with preconditions imposed at the gateway or by digital signature techniques, physical and organizational measures that can't be tracked through logs alone, or long-term attack scenarios that go beyond the time frame of the synthetic dataset. A significant avenue for future research involves expanding rule coverage as new regulations emerge. The third constraint is in the way the research was done. A pure rule-based method is less flexible than machine learning when it comes to dealing with behavior that is complicated or changing. However, it is clear and can be checked. You have to write and change rules by yourself if new patterns of violations come up. They might also have trouble capturing interactions between different features that weren't thought of during design. On the other hand, rule-based systems don't need big labeled datasets, and they make it easy to see how they relate to legal requirements, which is a big plus in a regulatory setting. In practice, a hybrid strategy that combines rule-based detection for clear compliance standards with anomaly detection methods for unexpected behavior may be the best way to go. Lastly, the current evaluation only looks at functional security outcomes (block/alert/integrity) and does not look at how well the system works in terms of reaction time, throughput, or resource use. These factors are essential for implementation in high-traffic clinical settings, particularly when real-time or near-real-time detection is necessary. In future work, they will need to be looked at again.

5.7 Scalability, internationalisation, usability for low tech users

Another major concern is how the system may be made bigger and fit into diverse regulatory environments. In this regard, the prototype's design is good. OPA is in charge of policy assessment. It loads rules from configuration files and can simply switch between multiple sets of rules. The log schema and policy model are broad enough to cover users, patients, resources, actions, and contextual aspects in many places. This makes it possible to support multi-jurisdiction operation by adding a configuration parameter that lets you choose the active

rule set. For example, you could choose between a Vietnam mode and an international mode that uses rules from frameworks like the European General Data Protection Regulation or the United States Health Insurance Portability and Accountability Act. This modular design also makes it easier to adapt to new AI healthcare compliance standards [26] and Zero-Trust frameworks for smart hospitals [22]. Also, users who aren't experts in security engineering or software development should be able to use the system. A lot of people who might use it are hospitals or clinics where the administrators can handle high-level setup but not change code or deal with complicated deployment procedures. To solve this problem, the thesis suggests an automatic update system that works like operating system updates. In this kind of setup, the vendor keeps an update server that has signed packages for new versions of the gateway, the SIEM backend, and rule sets. The SIEM dashboard would have a basic interface on the customer side, with buttons to check for updates and apply updates. When an administrator starts an update, the system would download the right package, check its signature, back up the existing configuration, apply the update, check for health issues, and automatically roll back if it finds a serious problem. This design would let customers with less technical know-how keep their systems patched and compliant without having to manually change the underlying containers or configuration files. In short, the discussion illustrates that the suggested system satisfies its high-level goals in a controlled experimental context and also reveals clear ways to make it better. The next chapter brings these ideas together to make general conclusions and specific goals for future work.

CHAPTER 6 - CONCLUSION AND FUTURE WORK

This chapter summarises the main contributions of the thesis, reflects on the extent to which the research questions have been answered, and outlines directions for future development of the proposed compliance monitoring system.

6.1 Summary of research contributions

The thesis's first contribution is the creation of a useful three-stream architecture for keeping an eye on compliance in electronic health record settings. Stream IAM/Gateway is made up of Keycloak, which is an identity and access management server; an NGINX-based gateway that uses OpenResty as the policy enforcement point; and OPA as the policy determination point. Stream EHR builds a prototype EHR system with FastAPI, React, and MariaDB. This shows how clinical workflows may be handled while also making extensive audit logs. Stream SIEM has a front end and a back end that collect, normalize, enrich, and analyze logs from the other parts. This architecture is made up of separate parts, leverages open source technology, and is designed to work with the limited resources of small and medium-sized healthcare facilities in Vietnam. The second contribution is a structured framework for converting Vietnamese

legislative requirements into technical regulations. The thesis develops a policy model by examining laws, decrees, and circulars pertaining to medical examinations, electronic health records, and personal data protection, thereby identifying pertinent entities, actions, and contextual elements. From this model, it creates a list of 196 rules that spell out specific logging needs, access controls, and behavioral limits. Each rule has a legal foundation, an explanation, the log fields needed for verification, and information on if and how it can be reviewed automatically. The third contribution is the creation and simulation of three high-impact attack scenarios (Brute-force, SQL Injection, and Log Tampering) to test the system's defenses. This goes beyond just checking rules to a "Red Team vs. Blue Team" test that shows the system can handle active threats. The fourth contribution is showing that a rule-based monitoring system made just for healthcare can strike a good balance between transparency, interpretability, and detection accuracy. The prototype demonstrates the feasibility of transcending theoretical talks of compliance to develop a functional system that enforces and monitors specific regulations established from legal frameworks.

6.2 Key achievements

The evaluation confirms that the proposed architecture successfully enforces a layered defense strategy. Specifically, the system demonstrated:

- Prevention: Successfully blocked brute-force attempts via IAM policies and SQL injection attacks via Gateway input validation.

- Detection: Generated real-time alerts for all attempts, ensuring immediate visibility for security operations.

- Integrity: Successfully detected unauthorized modification of audit logs through hash-chain verification, preserving the evidentiary value of the audit trail.

6.3 Research questions answered

The thesis presented three principal research inquiries. The first question was if it was possible to develop an automated compliance monitoring system for EHR environments in small and medium-sized healthcare facilities in Vietnam. The architecture, implementation, and evaluation discussed in the previous chapters demonstrate that this is certainly feasible. The prototype works on regular hardware, uses open source software, and can be set up with typical container tools. The second question was about whether this kind of technology could find policy violations and assaults. The evaluation findings show that the monitoring part can find and warn about active attack vectors, such as attempts to steal someone's identity and choices for application-layer injections. The research verifies the system's integrity against a simulated Red Team, demonstrating that the selected open-source components (Keycloak, OPA) can be

integrated to provide a unified security framework. The final question was about whether the system is appropriate for the way Vietnamese healthcare providers work and the rules they have to follow. The thesis answers positively by employing Vietnamese laws and decrees as the basis for the rule library, a language and tools stack that local teams can maintain, and by designing for limited resources. But complete appropriateness will depend on more testing in real hospitals and more work to make it easier for administrators and doctors to use.

6.4 Limitations

Despite these positive results, the research still has several important limitations that must be acknowledged. The primary constraint is the utilization of synthetic data for assessment. Simulated data provide accurate management of ground truth labels and mitigate privacy issues; nonetheless, they fail to encapsulate the complexity and unpredictability inherent in actual clinical activities. Consequently, the published performance measures may not align with those observed in actuality. The thesis regards the data as preliminary indicators of feasibility rather than conclusive assurances. A second limitation has to do with the range of rule implementation. The system implements 196 compliance rules covering Vietnamese healthcare regulations including Circular 54/2017/TT-BYT, Decree 13/2023/NĐ-CP. These rules were chosen to be representative and useful in real life, however they only cover a small part of the whole regulatory landscape. Adding more of the rule library to the system will take a lot of work in data modeling, policy writing, and testing. The third issue is that the thesis does not look at how well the system works in terms of reaction time, throughput, resource use, and scalability. These features are very important for a production deployment, especially if the system needs to look at logs in real time or support a lot of users at once. It is impossible to make significant assertions about the biggest installations that the prototype can handle without these dimensions. Another problem is that it's hard to use. To use the present setup, you need to know how to use Docker, configuration files, and log structures. It doesn't have a graphical interface for managing rules, and it doesn't have a built-in way to check and apply updates. This would be a hurdle to adoption for consumers who aren't very tech-savvy or small clinics who don't have their own IT team. Finally, the thesis does not compare the prototype to commercial SIEM products or to other methods, such as anomaly detection based just on machine learning or integrity solutions based on blockchain [23], [30]. These kinds of comparisons would assist put the suggested solution in the context of other security measures.

6.5 Future work

You can divide future work into three groups: short-term, medium-term, and long-term. The most critical thing to do in the short term is to test the system on genuine logs from partner hospitals that have been anonymized and are subject to strong privacy and ethical restrictions. This would let you change the detection criteria and thresholds based on how people really act, and it would also show you new edge cases that the synthetic dataset doesn't cover. At the same

time, the 196 implemented rules should be continuously validated and refined based on real-world feedback, focusing on rules that have a big influence on compliance and clear patterns for automatic detection. Adding more logs to the evaluation dataset, up to several thousand, would make the statistical analysis stronger. Short-term work should also include a comprehensive review of performance measures like response time and throughput. Crucially, future work must prioritize Human-Centric Security by conducting User Acceptance Testing (UAT) with frontline medical staff to evaluate operational friction. The goal is to verify that security interventions (such as break-glass prompts or re-authentication requests) do not introduce unacceptable delays to clinical workflows. This ensures that the system protects patient data without compromising the efficiency of care delivery. In the medium term, the 196 implemented rules should be maintained and updated as regulations evolve. You can put each rule into one of three groups: fully automatable, semi-automatable, or manual. This depends on whether you can check it from logs alone, if it needs more context or a human review, or if it can only be checked through periodic audits. A priority matrix that looks at how much of an effect a rule has and how easy it is to find would help you select which rules to put into place first. The automated updating mechanism described in Chapter 5 should also be turned into a working part at the same time. This features a central update server, an update client built into the SIEM dashboard, safe distribution of signed update packages, and the ability to automatically roll back changes. Another major medium-term goal is to make it easier for people from different countries and regions to work together. The same platform could be used in places with different legal systems, like the European General Data Protection Regulation or the United States Health Insurance Portability and Accountability Act, as well as new rules for AI governance in healthcare [26]. This is possible because rules are grouped into sets based on jurisdiction and the active set can be chosen through configuration. It would be even better if the user interface could be localized and compliance reports that were specific to each jurisdiction could be made. You may also improve the monitoring capabilities by adding machine learning techniques to the rule-based approach. For instance, anomaly detection algorithms could be trained using enhanced log data to identify unexpected behavior that doesn't break any rules but could signal new threats. A hybrid approach that uses both rule triggers and anomaly scores might be able to cover more ground without losing transparency. In the medium term, we also want to be able to process streaming logs in real time, connect with the HL7 FHIR AuditEvent standard, and do systematic usability testing with real administrators. In the long run, the architecture can be expanded to accommodate multi-hospital deployments, wherein a central monitoring service correlates occurrences across multiple institutions while adhering to data protection regulations. Predictive analytics can assist in figuring out how risky an account or department is and advise specific restrictions. Using blockchain-based methods, it would be possible to make audit trails that are hard to change and have great evidentiary value. Automated reporting modules could make compliance reports on a regular basis and send them to regulators. Lastly, a cloud native deployment architecture that works in multiple regions might make the system a managed service that many healthcare providers could use.

6.6 Final remarks

This thesis has shown that a rule-based, legally sound compliance monitoring system for electronic health records is both technically possible and practically useful for small and medium-sized healthcare facilities in Vietnam. The work goes beyond theoretical debates and provides a real solution that can be tested and improved by merging common identity and access management tools, a gateway-centric enforcement approach, a prototype EHR system, and a dedicated SIEM layer. The results, especially the successful denial of identity threats and the reliable detection of audit manipulation, show that the system is a good fit for places where security visibility is very important and staff resources are limited. The report also explicitly talks about the problems with synthetic data, limited rule coverage, performance measurement, and usability. These constraints don't make the contribution weaker; instead, they give a clear and honest plan for more research. If the system keeps getting better in the ways suggested in this chapter, especially in terms of real-world testing, automated updates, broader rule coverage, and internationalization, it could become a strong platform for monitoring compliance with regulations in healthcare and maybe even in other areas where sensitive data and complicated rules meet.

REFERENCES

[1] Ministry of Health Vietnam. (2018). *Circular No. 46/2018/TT-BYT on Electronic Medical Records*.

https://vbpl.vn/boyte/Pages/vbpq-toanvan.aspx?ItemID=137209&Keyword=

[2] Government of Vietnam. (2023). *Decree No. 13/2023/ND-CP on Personal Data Protection*.

https://xaydungchinhsach.chinhphu.vn/nghi-dinh-so-13-2023-nd-cp-bao-ve-quyen-du-lieu-ca-nhan-ngan-chan-cac-hanh-vi-xam-pham-du-lieu-ca-nhan-119230513100359528.htm

[3] National Assembly of Vietnam. (2023). *Law on Medical Examination and Treatment No. 15/2023/QH15*.

https://vanban.chinhphu.vn/?pageid=27160&docid=207396

[4] VnEconomy. (2025). *Ho Chi Minh City: Over 93% of hospitals have implemented electronic medical records*

https://vneconomy.vn/100-benh-vien-cong-lap-tphcm-trien-khai-benh-an-dien-tu.htm

[5] Nhan Dan Newspaper. (2024). *Implementing electronic medical records: Many barriers remain*.

https://nhandan.vn/tang-toc-trien-khai-benh-an-dien-tu-post908095.html

[6] NIST. (2020). *Attribute-Based Access Control (ABAC)*. Computer Security Resource Center.

https://csrc.nist.gov/glossary/term/attribute_based_access_control

[7] ScienceDirect. (2024). *Access control models for cloud-enabled electronic health records: A review*.

https://www.sciencedirect.com/topics/computer-science/attribute-based-access-control

[8] Ullah, F., et al. (2024). *Blockchain-enabled EHR access auditing: Enhancing healthcare data security*. PMC.

https://pmc.ncbi.nlm.nih.gov/articles/PMC11381610/

[9] Cobrado, U. N., et al. (2024). *Access control solutions in electronic health record systems: a systematic literature review*. ScienceDirect.

https://www.sciencedirect.com/science/article/pii/S2352914824001084

[10] arXiv. (2024). *GPT, Ontology, and CAABAC: Personalized Access Control Model*.

https://doi.org/10.48550/arXiv.2403.08264

[11] Journal of Medical Systems. (2024). *Automating Compliance in Healthcare: Case Studies of AI/ML Compliance*.

https://ijetcsit.org/index.php/ijetcsit/article/download/135/109

[12] AHIMA. (2023). *Audit Logs in Healthcare: A Critical Component of Investigation*.

https://journal.ahima.org/Portals/0/archives/AHIMA%20files/Privacy%20and%20Security%20Audits%20of%20Electronic%20Health%20Information%20(2013%20update).pdf

[13] HL7 International. *HL7 FHIR Release 4: AuditEvent Resource*.

https://hl7.org/fhir/R4/auditevent.html

[14] IEEE. (2022). *Rule-Based Systems for Compliance Checking in Healthcare*.

https://www.researchgate.net/publication/396166367_Comparative_Analysis_of_Rule-Based_Systems_and_AI-Driven_Approaches_in_Prior_Authorization_for_Healthcare_Services

[15] Computers, MDPI. (2024). *Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review*.

https://doi.org/10.3390/computers13020041

[16] Springer. (2024). *Privacy in Electronic Health Records: A Systematic Mapping Study*.

https://link.springer.com/article/10.1007/s10389-022-01795-z

[17] ResearchGate. (2024). *A Systematic Review of Security, Privacy, and Compliance Challenges in Electronic Health Records*.

https://www.researchgate.net/publication/392502161_A_Systematic_Review_of_Security_Privacy_and_Compliance_Challenges_in_Electronic_Health_Records_Current_Practices_and_Future_Directions

[18] ScienceDirect. (2020). *Security and Privacy of Electronic Health Records: Concerns, Barriers, and Solutions*.

https://doi.org/10.1016/j.eij.2020.07.003

[19] IJETCSIT. (2024). *Automating Compliance in Healthcare: Tools and Techniques*.

https://doi.org/10.63282/3050-9246.IJETCSIT-V2I3P105

[20] IEEE Access. (2025). *A Systematic Review of Access Control Models: Background, Existing Research, and Challenges*.

https://ieeexplore.ieee.org/iel8/6287639/10820123/10850915.pdf

[21] ResearchGate. (2025). *A Hybrid AI Framework for Detecting Insider Threats in Hospital Information Systems*.

https://www.researchgate.net/publication/398453610_A_Hybrid_AI_Framework_for_Detecting_Insider_Threats_in_Hospital_Information_Systems

[22] Archives of Current Research International. (2025). *Zero-Trust Architecture for Smart Hospitals: A Virtual Blueprint for Cyber-resilient Healthcare Infrastructure*.

https://www.researchgate.net/publication/396454594_Zero-Trust_Architecture_for_Smart_Hospitals_A_Virtual_Blueprint_for_Cyber-resilient_Healthcare_Infrastructure

[23] TandF Online. (2025). *Enhancing healthcare records management: a blockchain-based approach*.

https://www.researchgate.net/publication/397784308_Enhancing_healthcare_records_management_a_blockchain-based_system_for_secure_and_efficient_handling_of_electronic_health_records

[24] ResearchGate. (2025). *Predictive Modeling of Insider Threats in Healthcare Using Machine Learning*.

https://www.researchgate.net/publication/398118118_Predictive_Modeling_of_Insider_Threats_in_Healthcare_Using_Machine_Learning

[25] Al-Otaibi, S., & Al-Zahrani, F. A. (2025). "Enhancing Healthcare Security: A Unified RBAC and ABAC Risk-Aware Access Control Approach," *Future Internet*, vol. 17, no. 6, p. 262.

https://www.mdpi.com/1999-5903/17/6/262

[26] Liu, Z., Zhang, X., Xiao, B. (2024). "A Secure and Reliable Blockchain-based Audit Log System," in *IEEE International Conference on Communications (ICC)*.

https://ieeexplore.ieee.org/document/10623012

[27] Frontiers in Public Health. (2024). *A medical big data access control model based on smart contracts and risk*.

https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2024.1358184/full

[28] Hu, V. C., Ferraiolo, D., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations* (NIST Special Publication 800-162). National Institute of Standards and Technology.

https://doi.org/10.6028/NIST.SP.800-162

[29] ResearchGate. (2024). *SmartAccess: Attribute-Based Access Control System for Medical Records*.

https://www.researchgate.net/publication/365116370_SmartAccess_Attribute-Based_Access_Control_System_for_Medical_Records_based_on_Smart_Contracts

[30] Deshmukh, S., & Khobragade, P. (2025). "Blockchain-Based Logging to Defeat Malicious Insiders," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), vol. 13, no. 4.

https://ijireeice.com/wp-content/uploads/2025/04/IJIREEICE.2025.134114.pdf