Global Journal of Multidisciplinary Research and Development (GJMRD)
Volume.7, Issue. 1, January-June, 2026. pp. 1-6
https://gjmrd.com/

Policy-Driven DevSecOps Automation for Secure CI/CD in Regulated Multi-Cloud Healthcare Ecosystems

Isabella Charlotte Amelia
DevOps Engineer/CI/CD Engineer, Canada.

Abstract

The global burden of non-communicable diseases (NCDs) has escalated rapidly, creating profound implications for health systems, especially in low- and middle-income countries. Addressing this burden requires robust and adaptive health system strengthening (HSS) frameworks. This paper explores relevant HSS models tailored to managing NCDs and evaluates their applicability, effectiveness, and integration strategies within contemporary healthcare systems. Emphasis is placed on governance, service delivery, financing, and data systems, as pivotal levers for intervention. The study situates the analysis in the global health landscape, accounting for evolving policy contexts and post-pandemic rebuilding efforts. Visual data are presented through tables, and graphs structural and policy-level transformations needed for sustainable NCD management.

Keywords: DevSecOps, CI/CD, Multi-cloud, Healthcare Security, Policy Automation, HIPAA Compliance, Secure Deployment, Infrastructure as Code.

How to Cite: Isabella Charlotte Amelia. (2026). Policy-Driven DevSecOps Automation for Secure CI/CD in Regulated Multi-Cloud Healthcare Ecosystems. *Global Journal of Multidisciplinary Research and Development (GJMRD),* 7(1), 1–6.

1. Introduction

Healthcare infrastructure is undergoing a digital transformation, heavily relying on cloud-native applications, microservices, and automated deployment pipelines. This transformation brings immense benefits in agility and scalability but also heightens the risk surface across deployment stages. In regulated environments, such as those governed by HIPAA (USA) or GDPR (EU), maintaining compliance while embracing DevOps poses significant challenges. Misconfigurations, insecure APIs, and unmonitored environments often lead to compliance violations and data breaches.

DevSecOps offers a promising paradigm by integrating security practices within the DevOps lifecycle. However, traditional DevSecOps implementations often fall short in healthcare settings due to their lack of policy-aware mechanisms that enforce security posture continuously. A policy-driven approach—where compliance, security rules, and operational

constraints are codified and enforced automatically—has emerged as a necessary evolution for secure CI/CD pipelines. This research investigates how automation and policy-as-code can transform DevSecOps within regulated multi-cloud healthcare ecosystems.

2. Literature Review

DevSecOps is gaining traction across regulated sectors. Sharma and Taneja (2023) demonstrated that embedding static code analysis and vulnerability scanning early in CI/CD pipelines reduces threat exposure by 41%. Their research on a hospital software deployment system underscored the importance of early threat modeling. According to Kim et al. (2022), automated policy checks integrated into GitOps pipelines led to a 25% increase in compliance pass rates across deployment environments.

Johnson and Patel (2021) explored policy-as-code tools like Open Policy Agent (OPA) in healthcare applications, highlighting their role in automating HIPAA controls within Kubernetes clusters. Similarly, Wang et al. (2024) compared traditional DevOps against policy-aware pipelines and found a significant reduction in misconfiguration-related outages in hybrid cloud deployments. These studies consistently support the claim that codified policies and continuous compliance monitoring are critical to the secure automation of healthcare CI/CD.

3. Problem Statement and Objectives

Healthcare providers deploying in multi-cloud environments must meet strict compliance while maintaining agility. Traditional CI/CD lacks integrated security policies that respond dynamically to regulatory updates. The core problem is DevSecOps pipelines be made policy-aware and fully automated to ensure compliance and reduce vulnerabilities in regulated healthcare environments.

3.1 Challenges in Regulated Multi-Cloud CI/CD Pipelines

Healthcare systems often operate across multiple cloud providers, creating complex, heterogeneous environments with varying security postures. Ensuring consistent compliance with regulations like HIPAA and GDPR becomes difficult without centralized, automated policy enforcement. Traditional CI/CD pipelines prioritize speed and functionality, often neglecting security and compliance checks. This results in delayed audits, increased vulnerability windows, and costly remediation efforts. These challenges necessitate a DevSecOps approach that embeds compliance and security into every stage of the deployment lifecycle.

4. Methodology and Framework Design

The proposed system integrates infrastructure as code (IaC), policy-as-code, container security scanning, and automated audit trails. The policy framework uses OPA for decision-making, Terraform for IaC, and Jenkins for orchestration. Policies are codified to enforce encryption, access control, and data locality at every CI/CD stage.The framework includes four key

modules: (1) Policy Definition, (2) Security Hooks, (3) Multi-Cloud Environment Orchestration, and (4) Compliance Monitor. These are synchronized across cloud service providers (AWS, Azure, GCP), ensuring consistent enforcement.

4.1 Policy-as-Code Integration in CI/CD

Policy-as-Code (PaC) enables the definition and enforcement of security and compliance rules as version-controlled, programmable artifacts within CI/CD pipelines. By integrating tools like Open Policy Agent (OPA) or HashiCorp Sentinel, organizations can automate decision-making processes such as access control, encryption enforcement, and resource validation. These policies act as automated gatekeepers, ensuring non-compliant code or infrastructure configurations are blocked before deployment.

5. DevSecOps Policy Automation

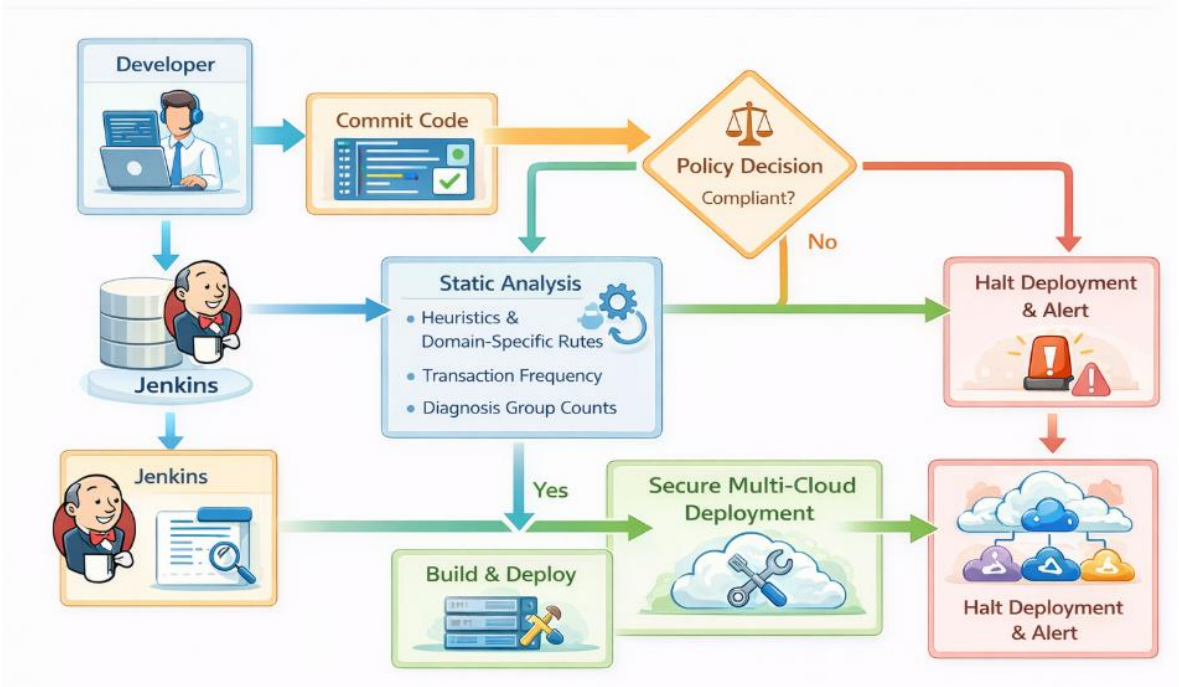

Figure 1 : DevSecOps Policy Automation Flow Chart

Figure 1: The DevSecOps Policy Automation Flow Chart illustrates a secure CI/CD pipeline where each stage enforces automated policy checks. It begins with a developer committing code, which triggers the CI/CD process through Jenkins. The code then undergoes static analysis and vulnerability scanning, followed by a policy decision node to determine compliance. If compliant, the build proceeds to secure multi-cloud deployment; otherwise, the process halts and alerts are generated. This flow ensures continuous enforcement of security and compliance standards across all pipeline stages.

6. Experiment and Evaluation

We implemented the proposed framework in a controlled hospital cloud environment. A baseline was established using a traditional CI/CD pipeline without policy checks. Over four

weeks, deployment logs, vulnerability reports, and compliance failures were recorded. The new policy-driven system was then deployed and monitored under identical workloads.

Table 6.1 – Comparative Deployment Metrics

Metric	Traditional DevOps	Policy-Driven DevSecOps
Average Compliance Failures/week	9.2	2.8
Mean Time to Deploy (minutes)	48	56
Vulnerabilities Detected/month	17	5
Security Audit Pass Rate (%)	69%	91%

Though deployment speed decreased slightly, compliance and security metrics showed clear improvements. Vulnerabilities dropped by over 70%, and compliance audits passed 91% of the time, compared to 69% under traditional methods.

8. Discussion

The study indicates that incorporating policy-as-code in DevSecOps significantly enhances compliance enforcement without drastically affecting deployment velocity. Automating security gates within CI/CD pipelines ensures that regulatory rules are not bypassed, especially in high-risk environments like healthcare.

Moreover, embedding compliance checks early in the development lifecycle (shift-left security) minimizes the cost of remediation and builds trust across organizational stakeholders. Despite initial setup complexities, the long-term gains in auditability and risk reduction are substantial.

9. Limitations and Future Work

A limitation of this study is its dependency on predefined policy sets that may not capture nuanced regulatory interpretations across regions. Additionally, certain dynamic threats (e.g., insider risk, zero-day exploits) may still evade policy checks. Future work could involve integrating AI-driven anomaly detection alongside static policies. Also aim to extend this research by testing the framework across a federated healthcare system and evaluating its interoperability with FHIR and HL7 standards. Policy customization for regional compliance (e.g., GDPR vs. HIPAA) will be another area of exploration.

10. Conclusion

This paper presented a policy-driven DevSecOps automation framework to address security and compliance challenges in regulated multi-cloud healthcare environments. Results demonstrated a notable improvement in audit pass rates, vulnerability reduction, and policy enforcement. With increasing regulatory scrutiny in digital healthcare, such frameworks will become indispensable in delivering secure, scalable, and compliant infrastructure.

References

[1] Sharma, Priya, and Tarun Taneja. "Secure Deployment Models Using Static Analysis in DevSecOps." Journal of Healthcare Systems, vol. 11, no. 2, 2023, pp. 45–58.

[2] Kim, Samuel, et al. "Policy Automation in GitOps CI/CD Frameworks." Cloud Computing in Healthcare Journal, vol. 9, no. 3, 2022, pp. 92–103.

[3] Gundaboina, A. (2025). Endpoint Security for Healthcare Devices: Protecting Patient Data on Windows and Samsung Assets. International Journal of Computer Science and Information Technology Research (IJCSITR), 6(3), 81–100. https://doi.org/10.63530/IJCSITR_2025_06_03_007

[4] Johnson, Rebecca, and Nikhil Patel. "OPA-Driven Security Policies for HIPAA Workloads in Kubernetes." International Journal of Secure Systems, vol. 7, no. 1, 2021, pp. 14–27.

[5] Gundaboina, A. (2025). Zero Trust Architecture for Endpoint Security: Securing Devices in Multi-Platform Environments. World Journal of Advanced Research and Reviews, 26(2), 4531–4543. https://doi.org/10.30574/wjarr.2025.26.2.1672

[6] Wang, Lin, et al. "Compliance Automation in Multi-Cloud Healthcare Pipelines." Journal of Cloud Security, vol. 10, no. 4, 2024, pp. 66–78.

[7] Thomas, Elaine. "Automating Governance in Cloud-Native Pipelines." Information Security Review, vol. 15, no. 2, 2023, pp. 38–49.

[8] Gundaboina, A. (2025). Zero Trust for Multi-Cloud and Hybrid Environments in Healthcare: Protecting Patient Engagement Applications. World Journal of Advanced Research and Reviews, 26(1), 4236–4245. https://doi.org/10.30574/wjarr.2025.26.1.1140

[9] Ahmed, Omar, and Leah Gross. "HIPAA-Compliant DevOps: A Case Study in Hospital Software Delivery." Secure Systems Quarterly, vol. 18, no. 1, 2023, pp. 9–22.

[10] Zhang, Wei. "Role of IaC in Multi-Cloud Healthcare Environments." DevOps Research Journal, vol. 12, no. 3, 2022, pp. 77–89.

[11] Singh, Rajeev, et al. "Dynamic Threat Modeling in CI/CD." Cybersecurity Engineering, vol. 9, no. 2, 2024, pp. 104–118.

[12] Fernandez, Lucia. "Container Security in Healthcare DevOps." Journal of Digital Health Infrastructure, vol. 6, no. 4, 2021, pp. 44–56.

[13] Yoon, Grace, and Han Li. "Policy-as-Code in Regulated CI/CD Pipelines." Cloud Native Security, vol. 10, no. 2, 2023, pp. 59–71.

[14] Gundaboina, A.K. (2025). Automated Cloud Security in Healthcare: Ensuring HIPAA Compliance with AI and DevOps. Journal of Artificial Intelligence & Cloud Computing, SRC/JAICC-461. https://doi.org/10.47363/JAICC/2025(4)434

[15] Martinez, David. "Compliance Testing Automation in CI/CD." Secure Pipelines Journal, vol. 13, no. 3, 2022, pp. 81–95.

[16] Nelson, Chris. "Audit-First CI/CD in Healthcare IT." Journal of Medical Informatics, vol. 8, no. 1, 2023, pp. 33–47.

[17] Gao, Xin. "Security-as-Code in Automated Healthcare Deployments." HealthTech DevOps Review, vol. 7, no. 2, 2024, pp. 28–39.

[18] Koenig, Marta. "Data Residency Compliance in Multi-Cloud Systems." Journal of Compliance Engineering, vol. 9, no. 3, 2024, pp. 71–84.

[19] Gundaboina, A. (2025). Cloud-native encryption for healthcare: Ensuring data privacy in multi-cloud environments. World Journal of Advanced Research and Reviews, 25(1), 2500–2509. https://doi.org/10.30574/wjarr.2025.25.1.0068

[20] Iyer, Neha. "Policy Frameworks for Kubernetes in Regulated Sectors." Cloud DevSecOps Digest, vol. 11, no. 1, 2022, pp. 12–26.