



REVIEW ON CLOUD AND DEVOPS INTEGRATION IN HEALTHCARE SYSTEMS

Dr. Malarkodi.KP', Aswitha. A², and Dharshini. A³

Assistant Professor, Department of Computer Applications, Sri Krishna College of arts and science, Coimbatore

^{2,3} Student III BCA-B, Department of Computer Applications, Sri Krishna College of arts and science, Coimbatore

Abstract

Healthcare organizations now sit in a weird and uncomfortable overlap: patients and clinicians expect software to evolve nearly all the time, while regulators like HIPAA and GDPR ask for data discipline, which quietly slows most development teams down. Cloud computing plus DevOps methods have turned into the two main pieces healthcare IT relies on to reduce that tension, cloud platforms provide scalable infrastructure that is compliance-certified, and DevOps supplies the automation needed so updates can be released safely and more frequently. This review brings together 15 papers released between 2023 and 2026 to check what the research really says when both ideas are used together, in real environments. It studies how DevOps is being adopted across healthcare organizations, how the same adoption shifts further into security-first DevSecOps once patient data is involved, how older hospital systems are being reshaped into cloud-native architectures, and how AWS, Azure, and GCP compare directly for healthcare workloads. It also looks at how DevOps thinking is being stretched into near real-time analytics for telehealth services and wearable devices. Overall the clearest theme across the literature is that healthcare-tailored DevOps is moving beyond “just automation”, toward continuous automated compliance and security examinations that are inserted into every pipeline step, not treated like an afterthought.

Keywords: Cloud Computing, DevOps, DevSecOps, Healthcare IT, Cloud-Native Architecture, CI/CD Pipeline, Microservices, Telehealth, IoT Healthcare, , Multi-Cloud Platforms, Healthcare Security, Automation, Kubernetes, Real-Time Health Analytics.

I. Introduction

For a long time, hospital IT systems were built with “stable first” as the main idea, you know big monolithic platforms that basically never changed because any change felt risky, even when it was needed. But that approach is starting to feel like it can't keep pace. Telehealth platforms, wearable health monitors, and patient portals now need frequent updates, just to stay aligned with new clinical guidelines, new devices, and the patient's expectations, and honestly none of that sits comfortably inside a slow, change-averse system. At the same time, it cannot get to the point where data protection gets loosened up, because healthcare data is covered by some of the strictest rules around, in basically every sense. So people keep



pointing to Cloud computing and DevOps, as the two technologies most often proposed to break the deadlock. Cloud platforms can give the elastic infrastructure plus the compliance certifications that healthcare organizations require, while DevOps, and its more security-hardened version DevSecOps, brings automation and a certain kind of operational discipline, so teams can deploy fast without losing governance control. This review kind of gathers together 15 papers from 2023 to 2026, and looks closely at how that pairing is playing out in practice. It checks where DevOps adoption stands today, how compliance is being automated in real workflows, how legacy systems are moving over to the cloud, how the major cloud providers compare specifically for healthcare, and how all of this extends into IoT and telehealth applications

Review

A. DevOps Adoption and Organizational Impact in Healthcare IT

The earliest wave of research in this area is mostly trying to prove that DevOps actually works in healthcare settings at all. You can see this in case-study evidence from big health systems, like Mayo Clinic, where DevOps adoption seems to make the flow of information more steady between clinical staff, and the IT teams [2]. A lot of that work also expects DevOps in healthcare to keep pace with broader cloud adoption since these two, tend to move together [2]. There's another strand of research that treats DevOps as just one part of a bigger three step change, sitting next to microservices architecture, and data visualization, and it argues that automating testing, configuration, and deployment reduces the kind of manual slip that healthcare just cannot really tolerate, almost more than any other industry. In that framing CI/CD pipelines help teams introduce new clinical guidelines or security updates far quicker than the old release rhythm allowed [3]. Some papers take the idea in a narrower way, for instance pairing cloud-based AI tools with Agile/SAFe delivery practices to automate healthcare call-center workflows and patient communication systems [4]. Cloud-native testing shows up in the same current too, with multiple papers describing testing frameworks that bundle automation, security checks, and AI-assisted validation into one pipeline phase rather than treating QA like it happens afterward [1]. Read as a set, these four papers basically suggest DevOps in healthcare shifting from being a pure tooling choice toward something more like an organizational habit, linked pretty directly to how quickly a hospital or provider is investing in cloud infrastructure [1][4].

B. DevSecOps and HIPAA/GDPR Compliance Automation

Once patient data enters the picture, the literature starts, to shift pretty noticeably from “DevOps” into “DevSecOps” and you can feel it in how people talk about pipelines. One detailed methodology paper lays out a kind of four-step DevSecOps framework, built specifically for patient engagement applications, and it even compares the approach directly against plain DevOps, then the takeaway is pretty direct: building security into each stage of the pipeline rather than treating it like an afterthought, at the end, measurably lowers organizational risk while also improving delivery speed and overall stability [6]. That

same paper also spells out what tools map to which stage, like static analysis tools such as SonarQube and Fortify that catch issues in source code before anything runs, dependency scanners like Snyk and WhiteSource that flag vulnerable open-source packages, dynamic analysis tools that probe the running application, and infrastructure-as-code scanning that spots misconfigurations in Terraform or Ansible templates before anything gets near production [6]. After deployment, continuous monitoring—SIEM platforms, intrusion detection, and behavior analytics—basically closes the loop, then what it finds gets fed back into the next planning cycle [6]. A companion paper goes one step further by putting AI on the compliance side, arguing that AI-assisted anomaly detection combined with DevSecOps practices removes a good chunk of the manual work required for HIPAA auditing, while still keeping PHI protection stronger and release velocity faster [8]. Broader cloud-security strategy work layers in zero-trust architecture and policy-as-code on top of the same general stack, and it also leans on AI-based anomaly detection for cloud-hosted healthcare data [9]. Taken together, this set of papers makes it clear that the healthcare DevOps conversation has moved well beyond basic CI/CD, it's now more like a security-first discipline, with compliance enforced by the pipeline itself.[6], [8], [9]. Figure 1 kind of shows how Cloud computing mixes with DevOps and DevSecOps inside today's healthcare systems. It points at secure cloud infrastructure, automated CI/CD routines, and telehealth services too, plus IoT-enabled medical devices that are always churning data in the background. Overall, it frames healthcare operations around compliance driven practices, like meeting policy, audits and all that.

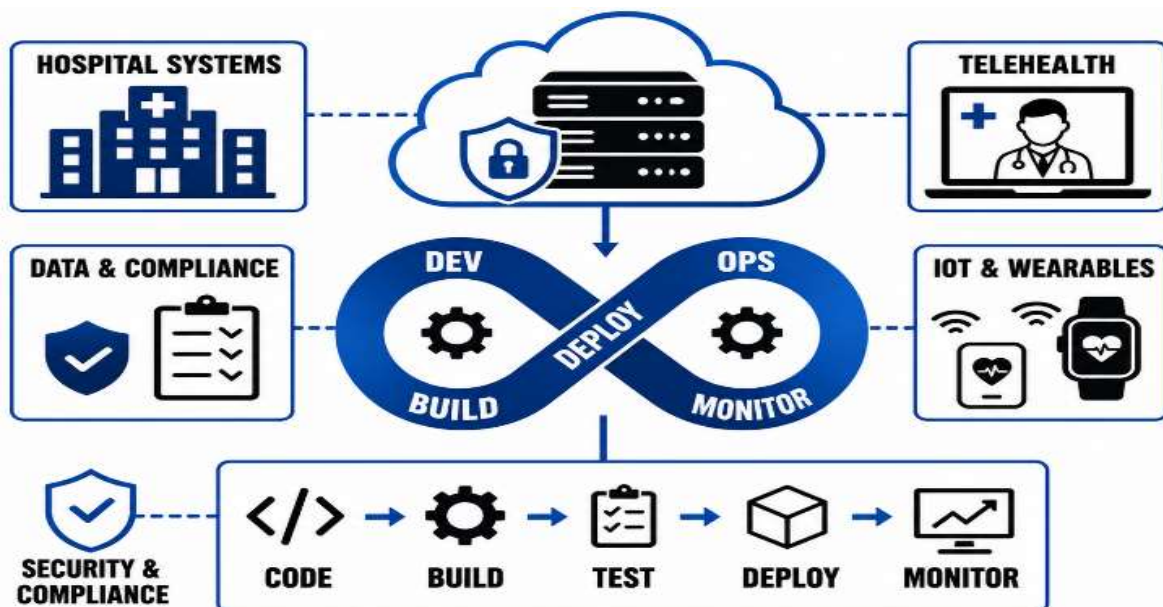


Figure 1. Cloud and DevOps Integration in Healthcare Systems

C. Cloud-Native Migration and Microservices Architecture



A third batch of papers tackles the tougher more practical issue, like actually shifting an old hospital setup into a cloud-native structure without letting anything get broken midstream. One migration-first paper talks about AI assisted tools for the transition and basically flags blue-green deployment as the preferred technique for keeping downtime almost at zero during cutover [10]. Then the devops best practice literature on tool picking sort of reinforces that, in a different way, suggesting Kubernetes-style orchestration because it can handle the weird, unpredictable demand surges that healthcare keeps running into, like outbreak spikes, flu season waves, and so on, without things falling apart on performance [7]. Other studies zoom out from one system and talk about the bigger ecosystem, using containerization, microservices and even serverless computing as methods to tie together EHRs, connected medical devices, and partner systems into a single cloud-native environment [11]. So regardless of whether you're modernizing just one legacy stack, or knitting together a broader multi system healthcare landscape, microservices plus container orchestration keep showing up as that shared architectural core [7], [10], [11].

D. Multi-Cloud Platform Comparison for Healthcare Workloads

A fourth theme basically lines up AWS, Azure, and GCP face-to-face, but not in that usual general cloud comparison way. it's more like, specifically through a healthcare lens, where you end up looking at architecture issues first. There they also mention that each provider, draws the shared-responsibility line a bit different, and then the "depth" of HIPAA-eligible services is not the same either. so the provider choice ends up shaping how a compliant architecture has to be designed , not merely which bill you pay [14]. Then the practical migration guidance throws in something most generic comparisons sort of skip entirely. even if you ignore HIPAA eligibility for a second, providers should still be judged based on FHIR and interoperability support. and also on how well they already fit with big EHR vendors like Epic and Cerner [15]. what this theme kind of makes obvious is that picking a cloud provider for healthcare isn't really a performance-and-cost call like it is in most other industries , it's much more tied to how far the compliance certifications go and how smoothly the provider works within the EHR ecosystem [14], [15].

E. DevOps for Real-Time Health Analytics, IoT, and Telehealth

The last theme takes DevOps out of core application delivery and basically puts it into faster moving, data-heavy situations. One framework is sort of centered on DevOps-driven pipeline patterns for real-time analytics on wearable IoT health data, and it argues that providers frequently skip automated DevOps-style deployment there even if these pipelines deal with the exact same scaling pressure as everything else in healthcare IT [12] A related enterprise framework pairs secure API design with embedded payment processing and then folds in DevOps practices inside a cloud-native setup, aiming for organization wide efficiency rather than only infrastructure [13]. Foundational telehealth research supports this, it points to the same three pillars you see in other sections too cost, DevOps-driven operational excellence, and security compliance as the deciding factors in cloud adoption for

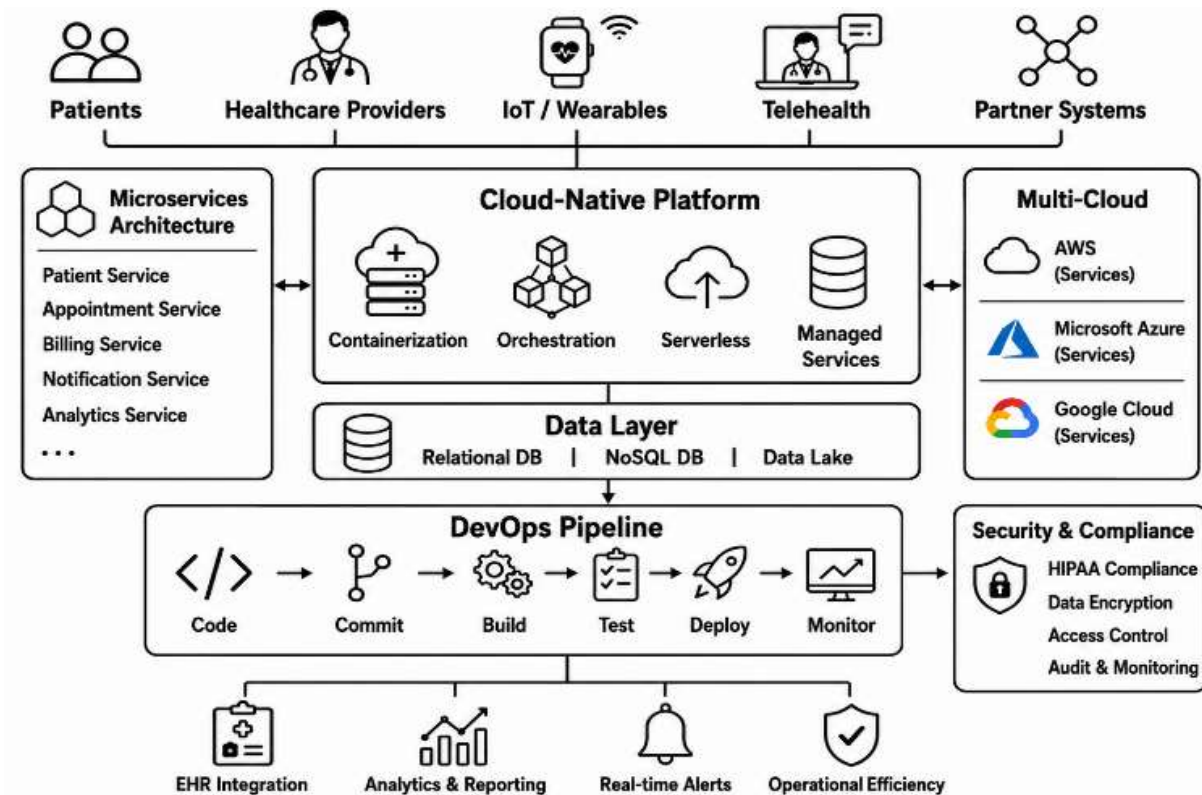


Figure 2. Qualitative Overview of Cloud-Native DevOps Adoption in Healthcare Systems

telehealth platforms specifically [5]. So across this theme, the takeaway is that DevOps's usefulness in healthcare doesn't just end at the core application layer, it flows pretty naturally into data pipelines and patient-facing services as well [5], [12], [13]. As Figure 2 shows

III. Comparative Analysis

Looked at side by side, all five themes point to the same underlying idea : cloud-native architecture plus CI/CD automation is this shared base that lets healthcare software move quicker, and security and regulatory compliance is the limitation that really determines which tools and platforms get built on top of that base [1]–[15]. The adoption-focused papers set up the business argument better collaboration, fewer manual mistakes for pushing DevOps at all [1]–[4]. The security-focused papers land right on top of that, basically showing DevSecOps rather than just plain DevOps is turning into the real standard once PHI enters the picture, with a fairly settled tooling stack spanning SAST, DAST, SCA and container/IaC scanning [6], [8], [9]. Then the migration papers converge on microservices and blue-green deployment as the technical approach that gets legacy systems onto this DevSecOps-ready base in the first place [7], [10], [11]. The provider-comparison papers go one step further, arguing that which cloud environment you pick is not really swappable for healthcare, because HIPAA-eligible service depth and EHR integration differ enough between AWS, Azure, and GCP to matter [14], [15]. And the application-layer papers also line up with that same stack, saying it rolls over cleanly into IoT analytics, telehealth, and patient-facing systems without requiring an entirely different toolset [5], [12], [13]. Figure 3 below gives a qualitative visual snapshot of how strongly each of the five review themes addresses five practical dimensions compliance automation deployment speed, migration complexity, multi-cloud flexibility, and IoT/real-time applicability. This synthesis is put together by the reviewer based on recurring patterns across the 15 papers, not numbers lifted straight out of any one source, and it should be read as an interpretive summary rather than a measured result.

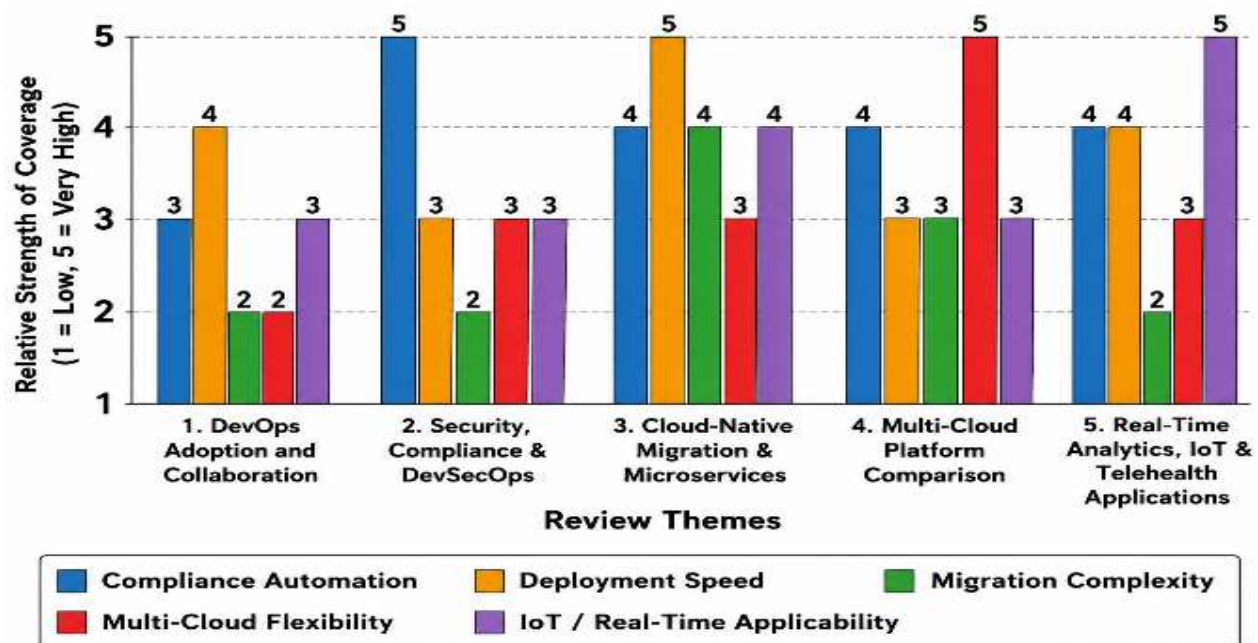


Figure 3 presents a qualitative comparison of the major review themes discussed in the study



IV. Future Research Directions

A couple gaps pop out across this bunch of papers. There still isn't some standardized way to benchmark DevSecOps tool stacks against each other, specifically for healthcare settings most papers just talk about tool groups like SAST and DAST without actually doing a head to head comparison [6], [8]. AI-assisted compliance automation is also stuck in that framework-proposal mode, not really proven at production scale, more than one time [8], [9]. And multi-cloud plus hybrid-cloud strategies where you use different providers side by side for distinct compliance requirements or EHR needs all at once seem underexplored compared to the kind of single-provider migration work described in [14], [15]. DevOps when it comes to real-time IoT health analytics is definitely moving, but it still feels pretty young, and you can tell more validation at real production scale is needed, not just concept demos [12]. Also as telehealth keeps growing, future research will probably have to shift toward DevOps for edge-deployed healthcare AI, like wearable inference, for example while still considering the cloud-centric practices this literature is mostly centered on today [5], [12].

V. Conclusion

Across all 15 papers, cloud computing and DevOps have, kind of, moved from "nice to have" efficiency tools to something close to essential infrastructure for healthcare software delivery. DevSecOps, not plain DevOps, looks like the better match specifically for healthcare workloads. The recurring finding is that building security and compliance inside the pipeline itself, rather than checking it afterward. This seems to reduce risk while still keeping delivery fast [6], [8], [9]. Cloud-native migration through microservices, plus blue-green deployment, gives the architectural footing this DevSecOps style really needs [7], [10], [11]. And the choice between AWS, Azure, and GCP should be driven more by HIPAA-eligible service depth and EHR ecosystem alignment, not just by headline performance numbers alone [14], [15]. The clearest open problems standardized DevSecOps benchmarking, production-validated AI compliance automation, and also tested multi-cloud compliance strategy. These are the most promising directions for where this research should go next [6], [8], [9], [14], [15].

References

- [1] B. B. Sudakara, "Integrating Cloud-Native Testing Frameworks with DevOps Pipelines for Healthcare Applications," International Journal of Research Publications in Engineering and Technology, 2023.
- [2] "Evaluating the Impact of DevOps Practice in the U.S. Health Care Systems," Journal of Knowledge Learning and Science Technology, vol. 2, no. 1, 2023.
- [3] "Transforming Healthcare: DevOps, Visualization, and Microservices," International Journals of Multidisciplinary Research Academy, 2023.



- [4] V. V. R. Boda, "AI Meets DevOps in Healthcare: Transforming How We Operate," International Journal of Artificial Intelligence, Data Science and Machine Learning, vol. 4, no. 3, pp. 10–17, 2023.
- [5] "DevOps for Telehealth Services: Accelerating Deployment and Scalability," ResearchGate preprint, 2024.
- [6] A. Gundaboina, "DevSecOps in Healthcare: Building Secure and Compliant Patient Engagement Applications," Frontiers in Computer Science and Information Technology (FCSIT), vol. 5, no. 2, pp. 17–37, 2024.
- [7] "Optimizing DevOps for Healthcare IT: Best Practices for Seamless Operations," MZ Computing Journal, vol. 2, no. 2, 2024.
- [8] "Automated Cloud Security in Healthcare: Ensuring HIPAA Compliance with AI and DevOps," Journal of Artificial Intelligence and Cloud Computing, 2025.
- [9] "Security and Compliance Strategies in Cloud-Based Healthcare Data Solutions," International Journal of Emerging Trends in Computer Science and IT (IJETCSIT), 2026.
- [10] "Migrating Legacy Healthcare Systems to Cloud-Native Microservices with AI: Best Practices and Pitfalls," ResearchGate preprint, 2025.
- [11] "Cloud-Native Integration Strategies for Healthcare Ecosystems," World Journal of Advanced Research and Reviews, vol. 26, no. 3, 2025.
- [12] J. M. I. Arockiasamy, "DevOps-Driven Real-Time Health Analytics: A Scalable Framework for Wearable IoT Data," International Journal for Multidisciplinary Research, 2025.
- [13] A. V. Barone, "Enterprise Real-Time Cloud Framework with Secure APIs, Unified Payments and DevOps Integration," International Journal of Engineering and Extended Research (IJEEFR), 2025.
- [14] "HIPAA-Compliant Cloud Architecture: AWS vs Azure vs GCP," Tactionsoft Technical Architecture Guide, 2026.
- [15] "Healthcare Cloud Migration: Step-by-Step Guide," Tactionsoft Technical Migration Guide, 2026.