

# A Safe and Compliant Roadmap for Healthcare IT at HealthSys

The recent 3-hour outage of HealthSys' hospital management software exposed critical gaps in system reliability, observability, and incident response

## Assessment & Cultural Shift .1

Begin with a cross-functional audit of infrastructure, deployments, and incident management. Establish a *DevSecOps* culture where development, operations, and compliance teams collaborate continuously, focusing on patient safety, uptime, and HIPAA compliance

## Infrastructure as Code (IaC) & Automation .2

Adopt IaC tools like Terraform or AWS CloudFormation to standardize environments across dev, staging, and production. CI/CD pipelines using Jenkins, GitLab, or GitHub Actions should enforce automated testing, security scanning, and deployment gates

## Observability & Monitoring .3

Implement centralized logging (e.g., ELK or Loki), monitoring (Prometheus + Grafana), and distributed tracing to gain visibility into system health. Define SLOs/SLAs to detect and respond to anomalies proactively

## Resilience & Disaster Recovery .4

Use blue-green or canary deployments to minimize downtime. Incorporate auto-healing, failover mechanisms, and regular DR drills. Store backups in encrypted, geographically redundant systems

## Security & Compliance Integration .5

Embed static/dynamic security scans, role-based access control, audit logs, and compliance checks into the pipeline. Leverage tools like HashiCorp Vault for secrets management and AWS Config for continuous compliance

## Continuous Improvement .6

After every release or incident, conduct postmortems and retrospectives. Continuously refine the pipeline based on real-world feedback and threat intelligence

With a compliant, resilient DevOps model, HealthSys can ensure its platform supports uninterrupted care delivery—safely and reliably