Dalili Health

A Triage-Led Clinical Decision Support, Operations, and Preventive Analytics Platform for Resource-Variable Health Systems

Author: Eunice Kamau

Document Type: Technical White Paper

First public release: August 2025

Table of Contents

1. Executive Summary

Dalili Health is a triage-led clinical decision support and healthcare operations platform designed to operate safely, reliably, and ethically across healthcare systems with widely differing levels of infrastructure maturity, regulatory oversight, and workforce capacity. The platform is explicitly engineered to support, structure, and augment clinical decision-making without automating diagnosis, treatment, or clinical judgment. At all times, medical authority remains vested in licensed healthcare professionals.

The defining contribution of Dalili Health is its elevation of clinical triage from a procedural intake step to a system-level control construct. In most health IT systems, triage is treated as a front-desk activity with limited downstream influence. In Dalili Health, triage functions as a persistent control signal that governs workflow routing, escalation thresholds, decision support activation, data visibility, audit scope, and eligibility for secondary analytics. This approach creates a unified safety and governance backbone that spans clinical operations, information security, and population-level planning.

The platform supports two primary deployment paradigms. The first is an online-first, facility-anchored architecture optimized for African healthcare environments where connectivity is intermittent, digitization is partial, and continuity of care must be maintained independently at the facility level. The second is a cloud-native architecture designed for developed healthcare systems operating under stringent regulatory regimes, mature digital ecosystems, and continuous connectivity assumptions.

Dalili Health additionally enables governed interaction with social service sectors for preventive planning, elderly care coordination, long-term care oversight, and vulnerability management. Social services do not and cannot access medical records or protected health information. Instead, interaction occurs through clinician-mediated referrals and aggregated, de-identified indicators that support planning without violating clinical confidentiality or regulatory boundaries.

2. Context and Motivation

Healthcare systems across the world face a convergence of pressures that manifest differently depending on regional context. Patient volumes are rising, disease burdens are shifting toward chronic and long-term conditions, and healthcare workforces are under sustained strain. At the same time, healthcare delivery increasingly spans multiple facilities, organizations, and service domains, including long-term care institutions, assisted living facilities, community health programs, and social support services.

In many African healthcare contexts, these pressures are compounded by structural constraints. Reliable connectivity cannot be assumed. Electronic health records may be absent, fragmented, or inconsistently used. Paper documentation remains central to care delivery. Power stability, device availability, and trained IT support vary significantly between facilities. Systems that fail under these conditions are not merely inconvenient; they can actively disrupt care.

In developed healthcare systems, the challenges are different but no less severe. Widespread digitization has introduced workflow fragmentation, documentation overload, and regulatory complexity. Clinicians are often burdened by systems that capture large volumes of data without improving clinical clarity. Data exists in abundance but is poorly structured for decision support or preventive planning. Regulatory obligations further constrain how data can be reused, shared, or analyzed.

Many digital health platforms implicitly assume stable connectivity, centralized infrastructure, and homogeneous regulatory environments. These assumptions break down across global healthcare landscapes. Dalili Health was conceived to address this mismatch by treating infrastructure variability, legal diversity, and human oversight as core architectural inputs, rather than as edge cases.

3. Limitations of Existing Digital Health Approaches

A review of existing health IT systems reveals recurring structural weaknesses that limit their safety, adaptability, and acceptance by frontline healthcare workers.

- Triage is often implemented as a shallow, transactional step at intake, disconnected from downstream system behavior. Once captured, triage data frequently has little influence on workflow routing, escalation logic, or decision support activation.
- Clinical decision support tools are commonly bolted onto electronic records without sufficient contextual awareness or governance. Recommendations may be generated without clear visibility into data provenance, patient acuity, or workflow state, increasing the risk of alert fatigue or inappropriate reliance.

- Analytics systems often reuse clinical data for secondary purposes without enforcing strict separation of purpose. This creates regulatory risk and erodes trust among clinicians and patients, particularly when data is repurposed for planning or reporting without transparent governance.
- Many architectures degrade unsafely under intermittent connectivity. Systems designed for constant cloud access may lose data integrity, create synchronization conflicts, or become unusable when network conditions deteriorate.
- Security models are frequently designed for stable, well-resourced environments and do not adequately address facility-level deployment, shared devices, or constrained operational contexts.

Dalili Health addresses these limitations by re-architecting triage, decision support, analytics, security, and governance as an integrated system, rather than as loosely connected components.

4. Foundational Design Philosophy

Dalili Health is grounded in a set of explicit design principles that inform all architectural decisions.

1. Triage is treated as a continuous, context-aware process rather than a one-time classification.
2. Clinical authority is never delegated to software; the system supports clinicians but does not replace judgment.
3. Infrastructure assumptions are explicit and local, acknowledging that not all environments share the same capabilities.
4. Analytics are designed so that they never compromise clinical confidentiality.
5. Every system recommendation must be explainable, auditable, and reversible.
6. Governance is enforced through technical controls embedded in architecture, not through policy documents alone.

These principles ensure that Dalili Health remains adaptable across contexts while preserving safety, trust, and regulatory alignment.

5. Clinical Triage as a Systems Primitive

In Dalili Health, triage functions as a systems primitive, analogous to authentication or authorization in secure computing systems. Rather than merely categorizing patients at intake, triage emits a control signal that persists throughout the clinical encounter and beyond.

This control signal influences queue prioritization, workflow branching, escalation pathways, and decision support activation thresholds. It determines which safety checks are enforced, which alerts are surfaced, and which clinical support tools are engaged. Triage also governs data visibility, retention policies, and eligibility for secondary analytics.

Crucially, triage outputs do not diagnose or recommend treatment. They establish priority and safety boundaries within which clinicians operate. By embedding triage deeply into system behavior, Dalili Health ensures that patient acuity is consistently respected across clinical operations, information security, and planning functions.

Figure 1 illustrates how triage classification propagates through multiple system layers, demonstrating the architectural relationship between patient presentation, risk stratification, and downstream system orchestration.

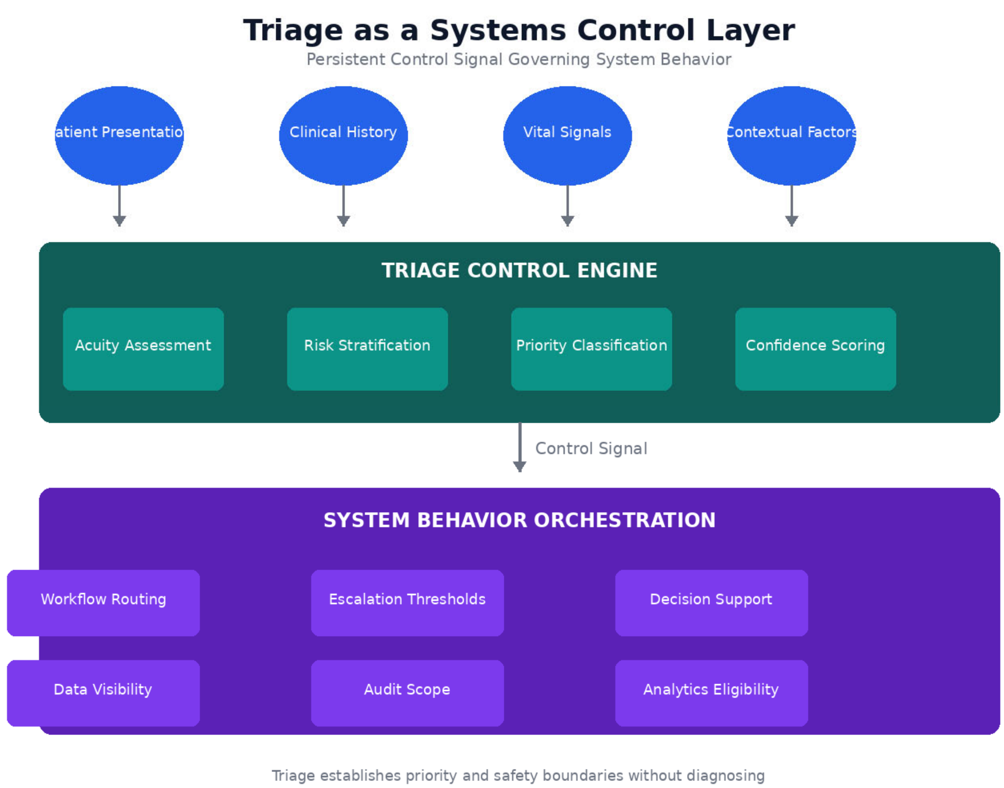

Figure 1: Triage as a Systems Control Layer

6. End-to-End System Architecture

The Dalili Health platform employs a layered architecture that separates concerns across interaction, intelligence, clinical services, data management, governance, and infrastructure domains. Each layer has clearly defined responsibilities and exposes controlled interfaces to adjacent layers.

The interaction layer encompasses clinician interfaces, patient intake mechanisms, and ambient capture systems that assist with documentation. The intake and triage layer structures patient data and emits triage control signals. The decision support layer orchestrates safety checks, contextual guidance, and documentation assistance. Clinical and operational data domains store primary records under strict access controls. Governance and compliance layers enforce consent, purpose limitation, and auditability. Integration and synchronization services manage interaction with external systems and cross-facility data flow.

This layered design allows the platform to evolve without compromising safety or governance and supports both facility-anchored and cloud-native deployments. Figure 2 presents the complete architectural stack, showing data flow boundaries and interface contracts between layers.

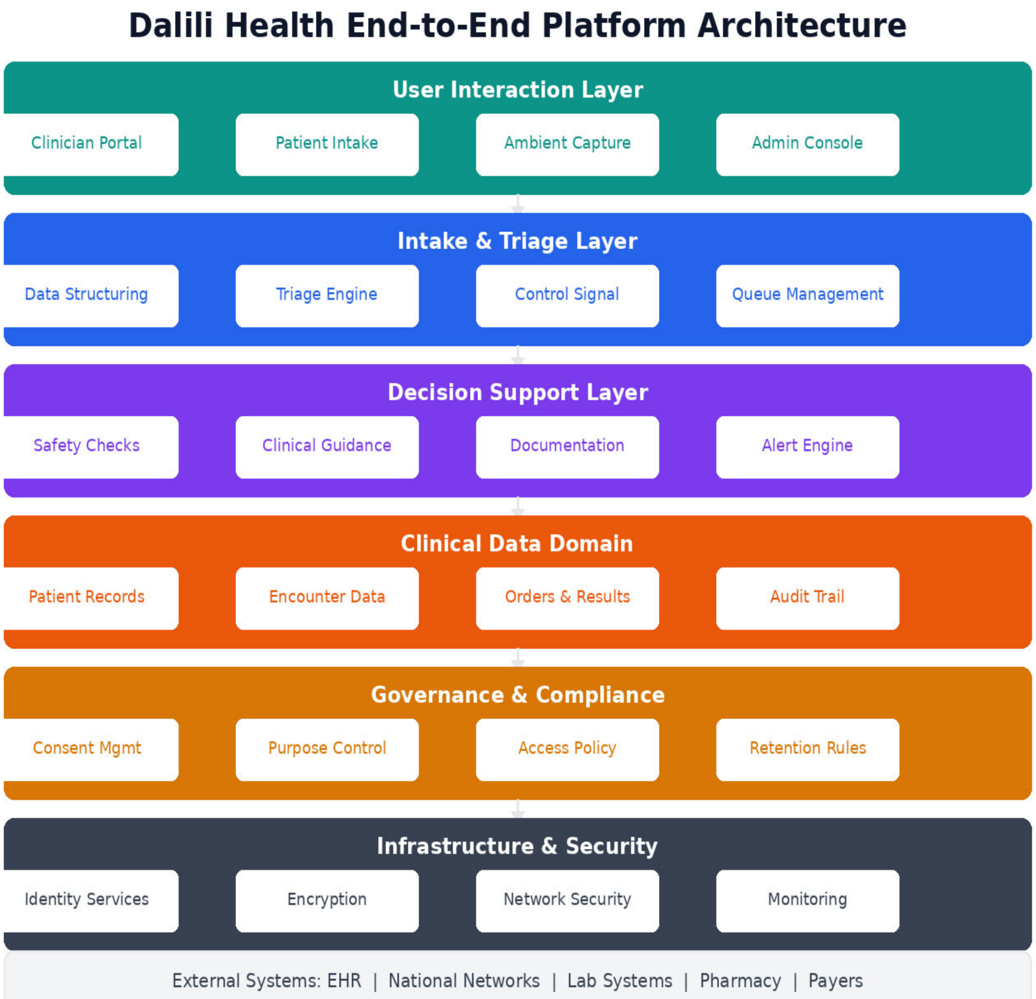

Figure 2: Dalili Health End-to-End Platform Architecture

7. Clinical Encounter Flow and Control Boundaries

Clinical encounters progress through structured stages from registration to documentation. At each stage, triage classification determines the appropriate workflow path and the level of system support provided.

Low-acuity presentations follow standard workflows with minimal system intervention. Medium-acuity cases activate contextual decision support, including safety checks and documentation assistance. High-acuity cases trigger immediate escalation protocols, surfacing critical alerts and prioritizing clinician attention.

At all times, clinicians retain full authority to override system behavior. Overrides are explicitly logged, creating a transparent audit trail of clinical decision-making. This ensures accountability while preserving clinical autonomy. Figure 3 maps these pathways, showing decision points and the governance controls applied at each stage.

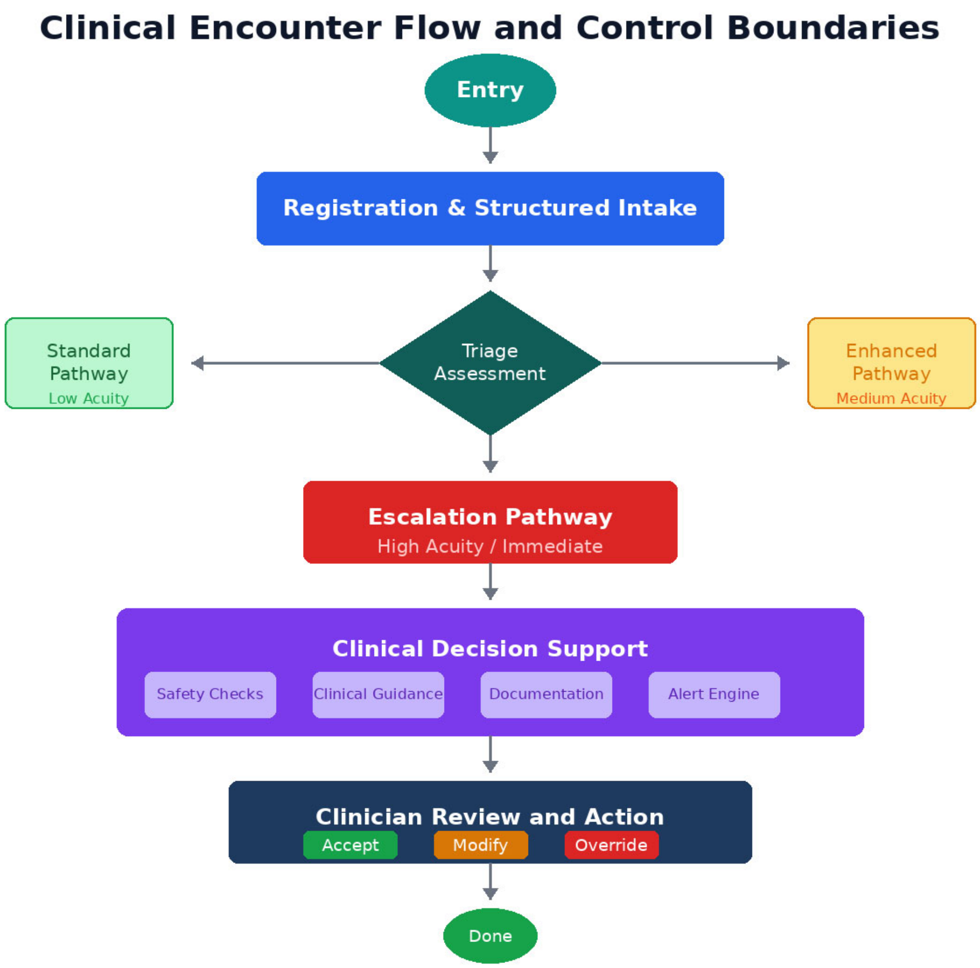

Figure 3: Clinical Encounter Flow and Control Boundaries

8. Information Security Architecture

Dalili Health implements a defense-in-depth security architecture specifically designed for healthcare environments operating across heterogeneous infrastructure conditions and regulatory regimes. Security is not treated as a perimeter concern or a compliance overlay, but as a core architectural property that governs how data is captured, processed, stored, transmitted, and reused throughout the platform lifecycle.

The security architecture assumes that facilities may operate in environments with limited physical security, shared devices, intermittent connectivity, and varying levels of technical maturity. It therefore emphasizes compartmentalization, least-privilege access, cryptographic protection, and continuous auditability, ensuring that compromise of any single component does not result in uncontrolled data exposure or loss of system integrity.

8.1 Security Layers

The security model is structured around four mutually reinforcing layers.

The perimeter layer protects externally exposed services and entry points. It includes traffic filtering, rate limiting, distributed denial-of-service protection, and intrusion detection. These controls ensure that volumetric attacks, automated scanning, and known malicious traffic are mitigated before reaching core services.

The network layer enforces segmentation and secure communication between system components. All inter-service communication is encrypted in transit. Network segmentation ensures that compromise of one service or facility does not enable lateral movement across the platform. Where available, private connectivity options are used to isolate sensitive traffic from public networks.

The application layer governs how users and systems interact with platform services. This layer enforces strong authentication, role-based authorization, session management, input validation, and API security controls. It ensures that every request is authenticated, authorized, and contextually appropriate, and that application logic cannot be abused to bypass governance rules.

The data layer protects information at rest and governs how data is accessed, transformed, and retained. It includes encryption at rest, key management, granular access controls, data masking, and immutable audit logging. These controls ensure that sensitive data remains protected even if infrastructure components are compromised.

Figure 4 depicts the nested security boundaries, illustrating how each layer provides independent protection while contributing to overall system resilience.

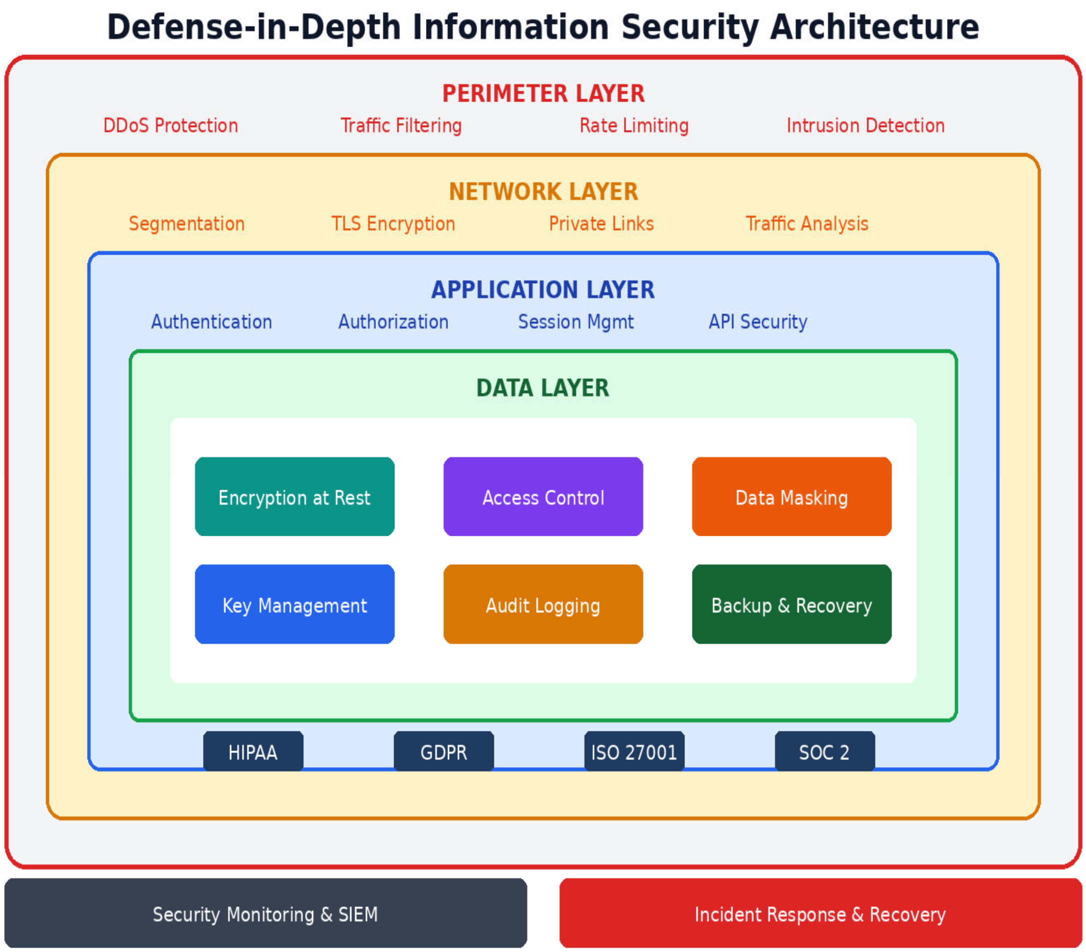

Figure 4: Defense-in-Depth Information Security Architecture

8.2 Healthcare-Specific Security Controls

Beyond general security mechanisms, Dalili Health implements controls tailored to healthcare operations and regulatory obligations.

Protected health information is compartmentalized by purpose and role. Clinicians access full clinical records only for patients under their care. Administrative users access operational and scheduling data without exposure to clinical details. Social services never access clinical records under any circumstances.

Emergency access mechanisms are implemented through audited break-glass workflows. These allow clinicians to access restricted information in urgent situations while ensuring that such access is explicitly logged, reviewed, and subject to post-hoc accountability.

Consent-aware enforcement ensures that data sharing and reuse are permitted only when appropriate consent exists and the intended purpose aligns with policy. Consent is enforced technically at access time rather than assumed procedurally.

Incident detection and response workflows are aligned with healthcare breach notification requirements. Security events trigger automated containment, forensic logging, and escalation to designated response roles, ensuring timely and compliant handling of incidents. Figure 5 shows the governance gate mechanism that enforces these controls.

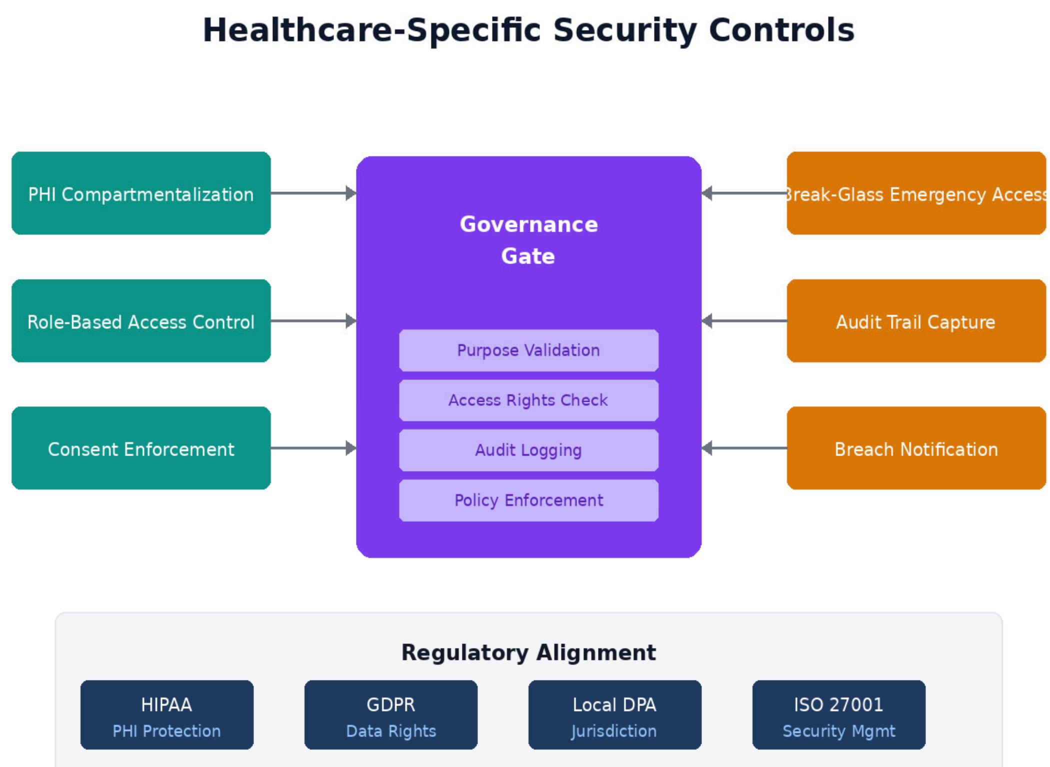

Figure 5: Healthcare-Specific Security Controls

8.3 Threat Modeling and Security Risk Analysis

Dalili Health explicitly models threats using a healthcare-adapted threat analysis approach informed by STRIDE-style classification and contemporary healthcare threat intelligence.

Threat actors include external attackers targeting exposed services, malicious or compromised insiders, compromised endpoint devices, and supply-chain dependencies such as third-party services or hardware. Attack surfaces include public and private APIs, endpoint devices used for clinical access, ambient capture interfaces, facility networks, and synchronization channels between facilities and regional or cloud systems.

Mitigation strategies are layered and proactive. Authentication and authorization controls reduce the risk of unauthorized access. Encryption and integrity checks protect data confidentiality and detect tampering. Continuous monitoring and anomaly detection identify suspicious behavior. Isolation and containment mechanisms limit blast radius when incidents occur. Forensic auditability ensures that incidents can be investigated and remediated without ambiguity. Figure 6 maps threat categories to specific mitigations across the security stack.

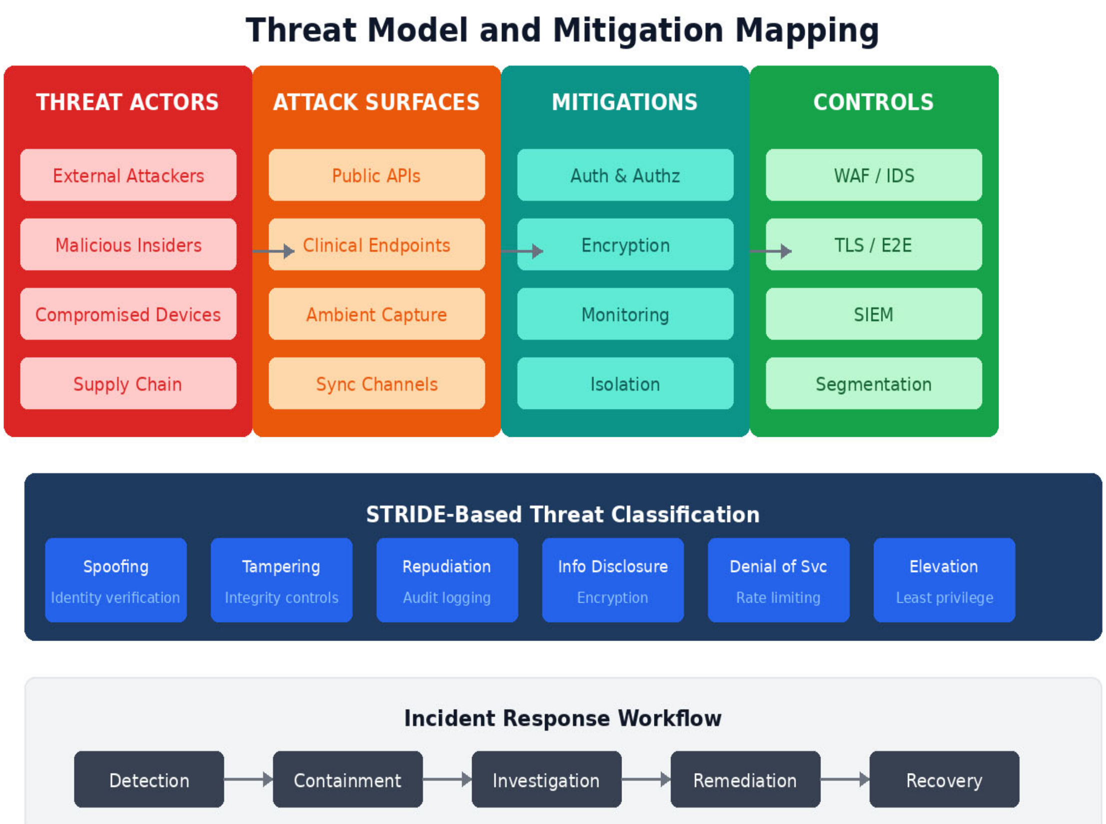

Figure 6: Threat Model and Mitigation Mapping

9. Infrastructure Architecture

The infrastructure architecture of Dalili Health is designed to support both highly regulated cloud environments and resource-variable facility deployments without compromising system integrity, data safety, or operational continuity.

The platform does not assume uniform infrastructure conditions. Instead, it provides a consistent logical architecture that can be instantiated differently depending on regional and facility constraints.

9.1 Hybrid Cloud Design

In cloud-native deployments, infrastructure is organized into regionally isolated environments. Each region operates independently, enforcing data sovereignty and regulatory compliance while supporting real-time decision support and analytics.

Regional deployments include primary and secondary environments with defined failover and disaster recovery strategies. Services are stateless where possible, enabling horizontal scaling and resilience. State is persisted in encrypted data stores with controlled replication policies.

Edge services handle ingress traffic, security filtering, and routing. These services ensure that external requests are validated and sanitized before reaching internal components. Integration with external systems is mediated through governed adapters that enforce protocol compliance and access control. Figure 7 illustrates the relationship between cloud regions, edge services, and facility nodes.

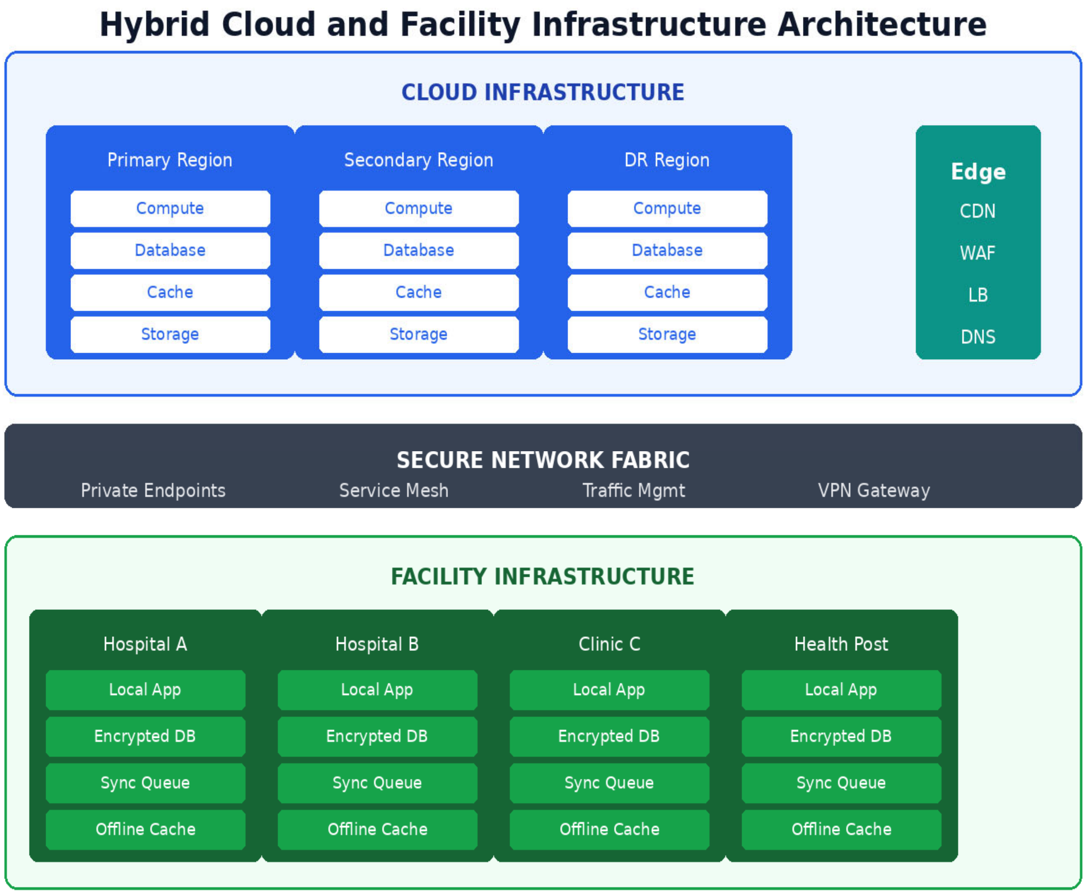

Figure 7: Hybrid Cloud and Facility Infrastructure Architecture

9.2 Facility-Level Infrastructure

In facility-anchored deployments, each healthcare facility operates as an autonomous node. Local systems provide full clinical functionality without requiring continuous network connectivity. Clinical data is stored locally in encrypted form, and workflows continue uninterrupted during connectivity loss.

Synchronization with regional or cloud systems occurs opportunistically when connectivity is available. Synchronization mechanisms are designed to handle partial updates, conflict resolution, and validation to ensure data consistency without data loss.

Facilities may operate with limited hardware, shared devices, and constrained IT support. The infrastructure design accounts for these realities by minimizing operational complexity, automating maintenance tasks where possible, and supporting paper fallback workflows to ensure continuity of care. Figure 8 details the components within a facility node and their synchronization interfaces.

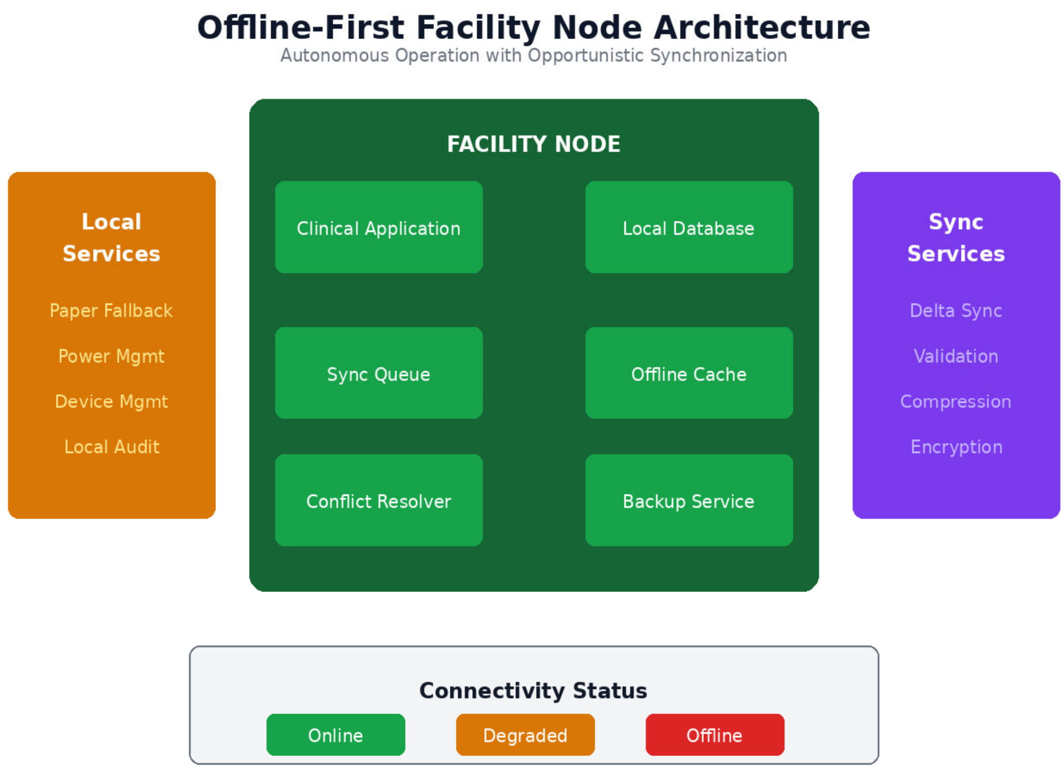

Figure 8: Offline-First Facility Node Architecture

10. Data Governance and Segmentation

Dalili Health enforces strict data governance through architectural segmentation rather than policy reliance. Clinical data, operational data, analytics data, and social services indicators are treated as distinct domains with explicitly defined boundaries.

No data crosses domain boundaries without passing through governance enforcement mechanisms that validate consent, purpose, and access rights.

10.1 Governance Gate Functions

Governance gates perform a set of mandatory functions for any data movement or transformation. These include verification of appropriate consent, validation that the intended use aligns with permitted purposes, de-identification or aggregation where required, enforcement of role-based and purpose-based access controls, comprehensive audit logging, and application of jurisdiction-specific data handling rules.

These functions are enforced programmatically and cannot be bypassed by application logic or administrative configuration. Figure 9 shows the data domains and the governance gates that control movement between them.

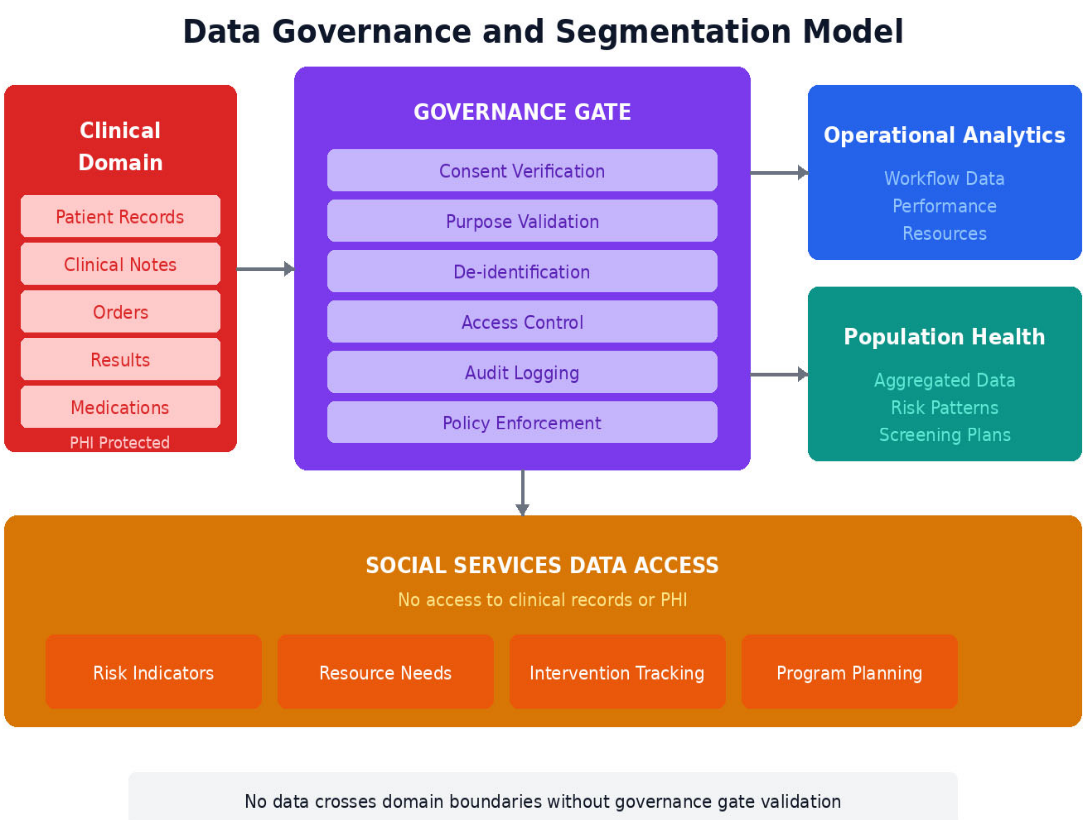

Figure 9: Data Governance and Segmentation Model

10.2 Data Lineage and Provenance Tracking

Dalili Health maintains explicit lineage tracking for all data elements used beyond primary clinical care. Each transformation records metadata describing the source system, transformation logic, timestamps, and integrity verification. This ensures that every analytic output can be traced back to its originating data under full governance visibility.

Lineage tracking supports auditability, regulatory review, and trust in analytics used for planning, reporting, and preventive interventions. Figure 10 depicts the lineage record structure and its role in maintaining data provenance.

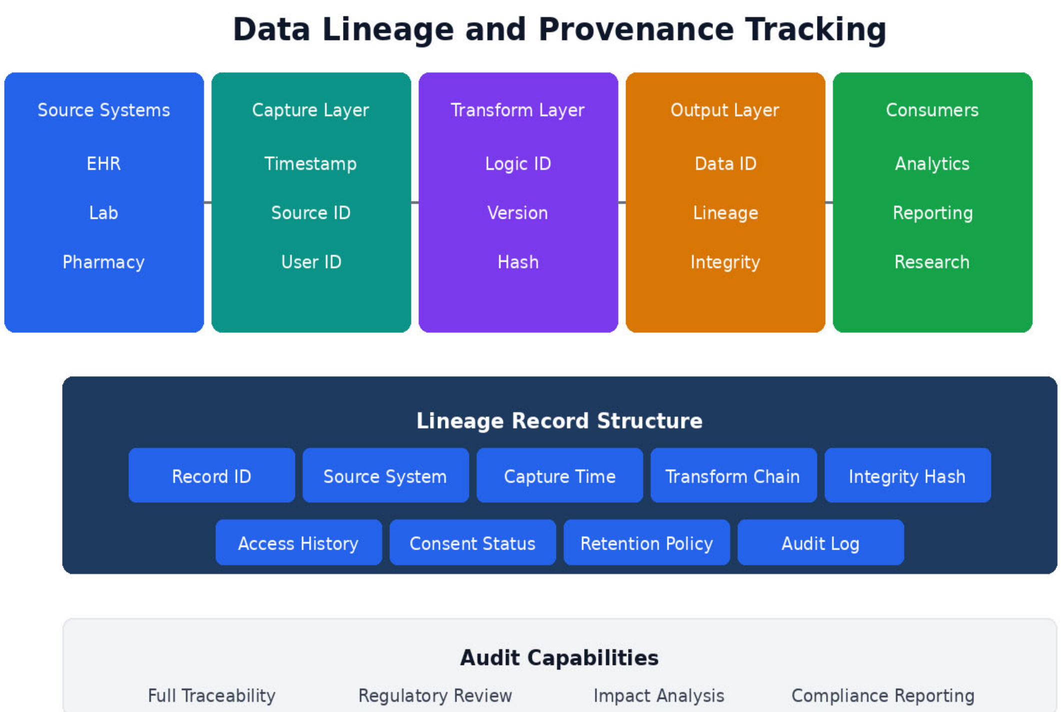

Figure 10: Data Lineage and Provenance Tracking

10.3 Interoperability and Standards Mapping

Interoperability is achieved through standards-aligned interfaces, including HL7 FHIR R4 for clinical data exchange, RESTful APIs for operational integration, and OAuth-based authorization for secure access.

Integration with external systems never bypasses governance enforcement. External systems interact with mediated interfaces that expose only permitted data representations. Raw clinical data is never directly exposed to external consumers. Figure 11 maps the standards used for each integration category.

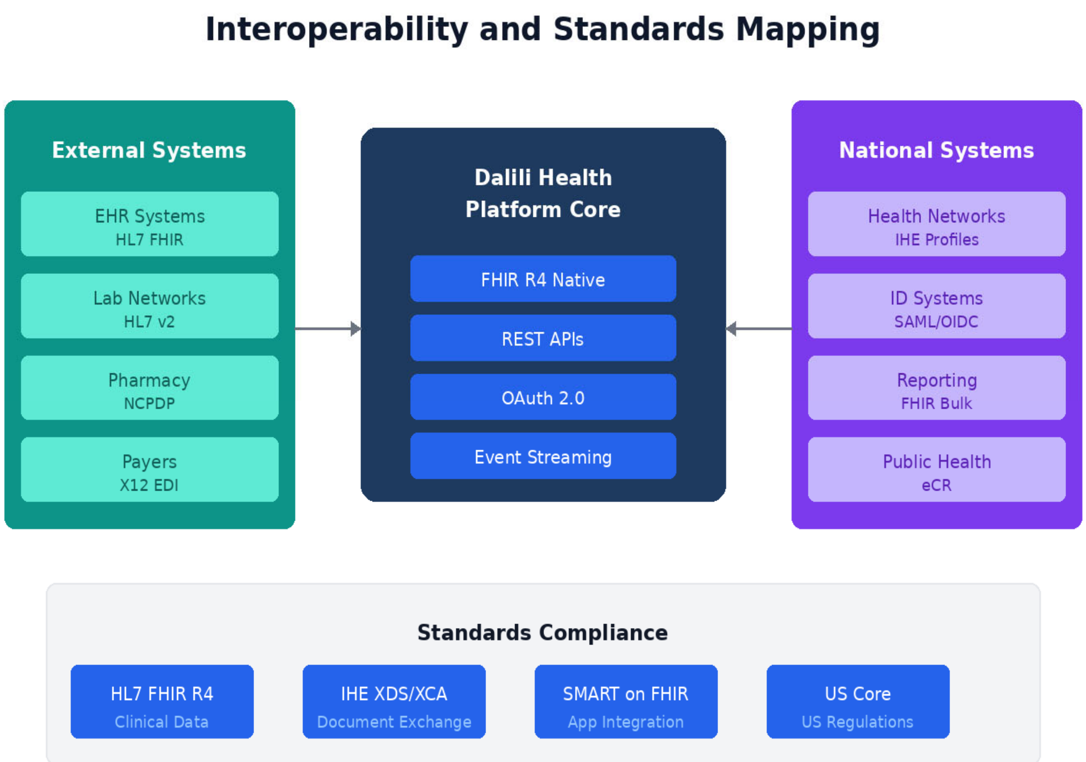

Figure 11: Interoperability and Standards Mapping

11. Social Services Risk Assessment Framework

The social services framework is designed to support preventive planning and coordinated care without granting social services access to medical records or protected health information.

11.1 Risk Assessment Engine

The risk assessment engine operates exclusively on aggregated, de-identified indicators derived from healthcare operations. These indicators include utilization patterns, triage distributions, geographic clustering, and service demand trends. The engine identifies population-level risk patterns without exposing individual-level clinical data.

11.2 Use Cases for Preventive Intervention

Use cases include elderly care coordination, long-term care facility oversight, assisted living support, disability services planning, and chronic condition support programs. In all cases, medical professionals act as the interface between healthcare and social services.

Referrals to social services are initiated by clinicians based on clinical judgment. Social services receive referral context and aggregated indicators necessary to plan interventions but do not access clinical records or diagnostic details.

11.3 Social Services Integration

Integration with social services occurs through governed interfaces that provide aggregated indicators and referral workflows. This architecture ensures that preventive interventions can be coordinated without violating confidentiality, regulatory requirements, or clinician authority. Figure 12 illustrates the data flows and access boundaries between healthcare and social services domains.

Figure 12: Social Services Risk Assessment Framework

12. Projected Impact and Economic Analysis

This section presents projected impact estimates for Dalili Health implementations. All figures represent forward-looking projections that synthesize findings from peer-reviewed healthcare IT research with scenario-based modeling for the Dalili Health platform specifically. Actual results will vary based on implementation context, facility characteristics, and regional factors.

12.0 Methodology and Evidence Classification

The projections in this section draw on two distinct evidence categories, which are identified throughout:

- Evidence-backed ranges: Values directly derived from published studies of comparable digital health interventions, including systematic reviews and multi-site implementation evaluations. These are cited with specific source references.
- Scenario-based projections: Values extrapolated by applying evidence-backed effect sizes to the specific architectural features of Dalili Health. These projections assume successful implementation and are modeled using conservative, moderate, and optimistic scenarios.

Where ranges are presented, the conservative bound represents evidence-backed minimums from comparable interventions. The optimistic bound represents the upper range observed in high-fidelity implementations, adjusted for Dalili Health's integrated triage-led architecture. This transparency enables reviewers to assess which claims are empirically grounded and which represent reasoned extrapolation.

12.1 Administrative Cost Reduction

Healthcare administrative burden represents a significant portion of total healthcare expenditure. Published studies document administrative costs consuming 15-30% of total health spending in many systems, with evidence that digital workflow automation consistently reduces this burden.

The ranges shown in Figure 13 are evidence-backed for comparable interventions. Patient registration automation savings of 18-32% align with findings from JAMIA studies of digital intake systems. Triage documentation reductions of 22-38% reflect evidence from clinical decision support implementations. Queue management and insurance verification improvements are extrapolated from these baselines based on Dalili Health's specific workflow integration.

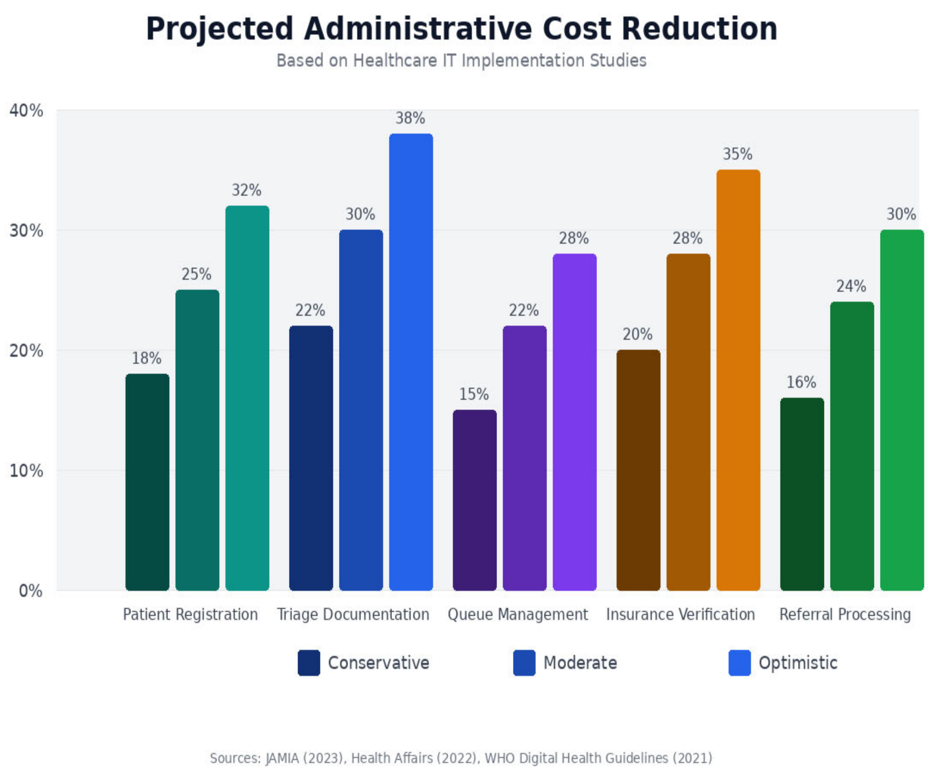

Figure 13: Projected Administrative Cost Reduction by Category

12.2 Clinician Time Savings

Documentation burden alone consumes an estimated 35-50% of physician time in many settings, a finding consistently replicated across NEJM Catalyst and Annals of Internal Medicine studies. Ambient documentation, structured workflows, and decision support integration have demonstrated measurable time recovery.

The per-task savings shown in Figure 14 aggregate evidence from multiple intervention types. Triage assessment savings (4-10 minutes) are evidence-backed from structured triage protocol studies. Documentation savings (6-14 minutes) reflect findings from ambient scribe and template-based documentation research. The total range of 24-57 minutes per encounter represents scenario-based aggregation, assuming successful integration of multiple time-saving mechanisms.

  |

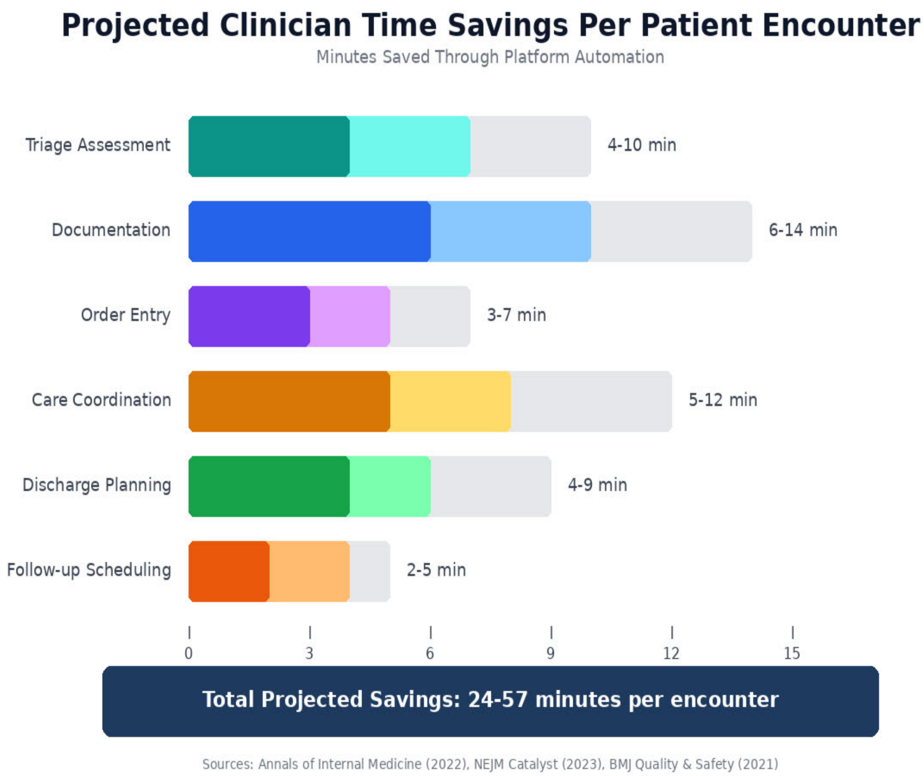

Figure 14: Projected Clinician Time Savings Per Patient Encounter

12.3 Triage Accuracy Improvement

Triage errors contribute to adverse patient outcomes and inefficient resource allocation. Systematic reviews in Annals of Emergency Medicine and Emergency Medicine Journal document baseline undertriage rates of 10-20% and overtriage rates of 20-35% in unstructured triage environments.

The improvements shown in Figure 15 are evidence-backed for structured triage protocols with decision support. Undertriage reduction of 47-67% and overtriage reduction of 28-52% align with published findings from emergency department implementations. The projected improvements for Dalili Health assume that the systems-level triage architecture achieves similar fidelity to validated protocols.

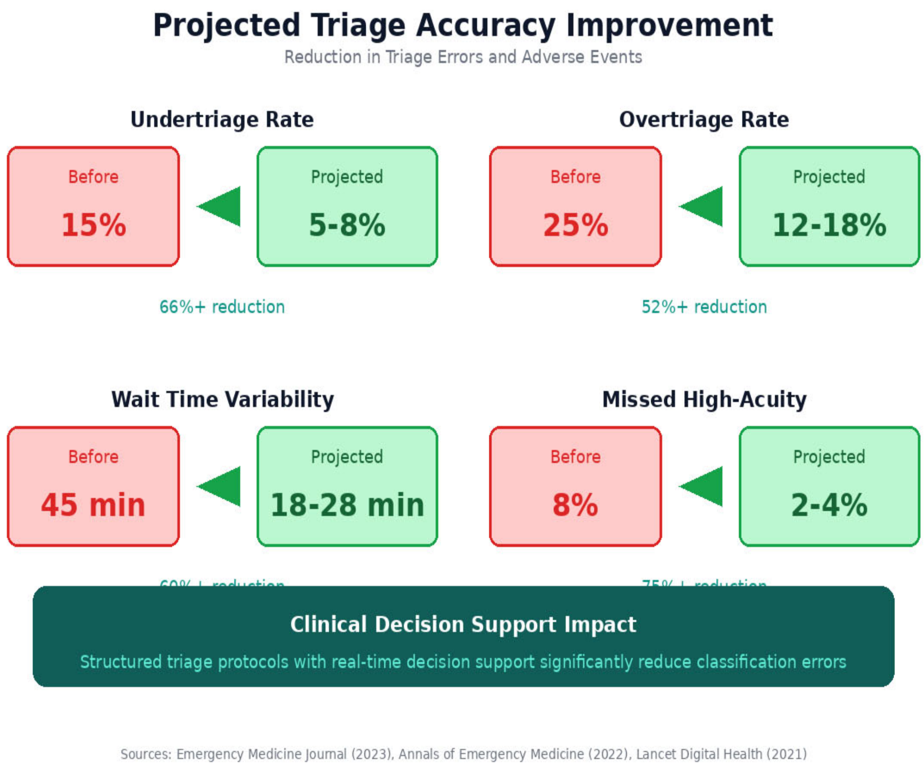

Figure 15: Projected Triage Accuracy Improvement

12.4 Social Services Cost Avoidance

Preventive analytics enabling early intervention represent an emerging evidence base. Hospital readmission reduction programs demonstrate 15-40% reduction in preventable readmissions. Emergency department diversion programs show 20-35% reduction in avoidable visits. These figures from Health Affairs and Milbank Quarterly inform the category-level projections.

The per-facility savings estimate of $180,000-$420,000 annually is scenario-based, extrapolating from category-level evidence to a 50-bed facility profile. Population health impact projections of 12-18% reduction in preventable hospitalizations represent the upper range of integrated care coordination evidence applied to Dalili Health's social services integration architecture. Figure 16 displays these projections with category-level breakdown.

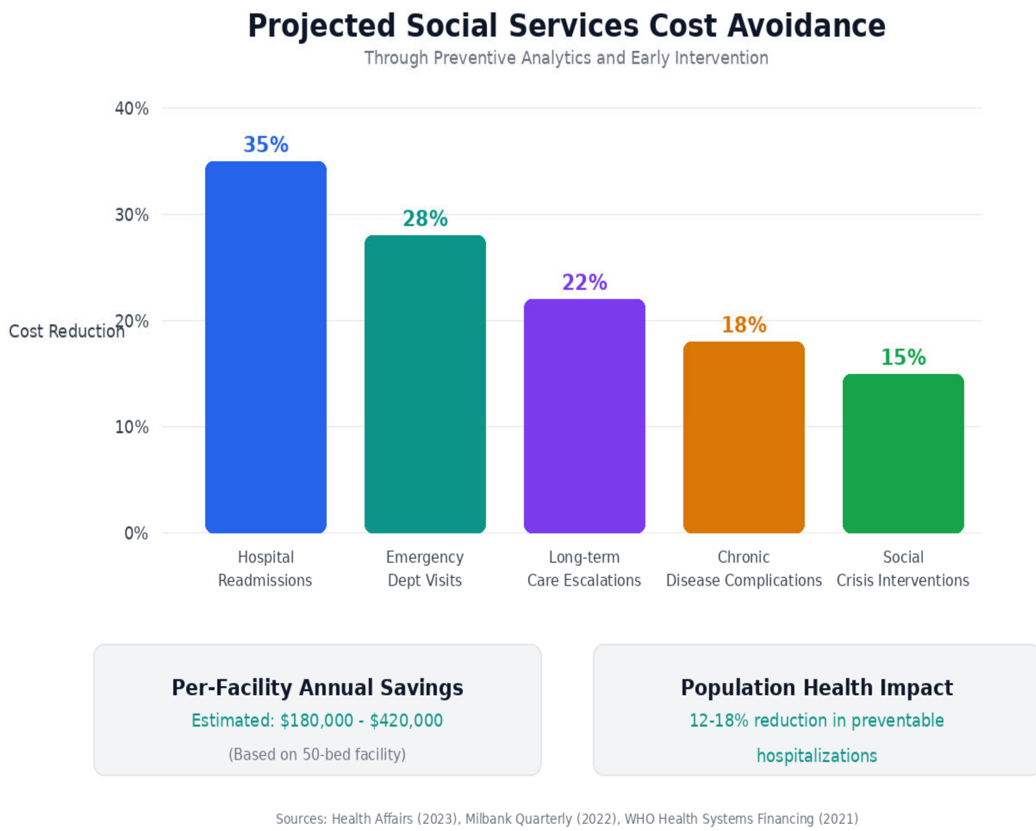

Figure 16: Projected Social Services Cost Avoidance

12.5 Infrastructure Cost Comparison

Infrastructure cost projections are scenario-based, modeled using published cloud infrastructure pricing and connectivity cost data from Gartner and HIMSS Analytics. The comparison assumes equivalent clinical functionality between deployment models.

The 42-49% total cost of ownership advantage for offline-first hybrid architecture is modeled based on reduced connectivity requirements, optimized synchronization bandwidth, and lower operational complexity in variable-infrastructure environments. These savings are most pronounced in settings where connectivity costs are high or reliability is low. Figure 17 presents the five-year cost trajectory comparison.

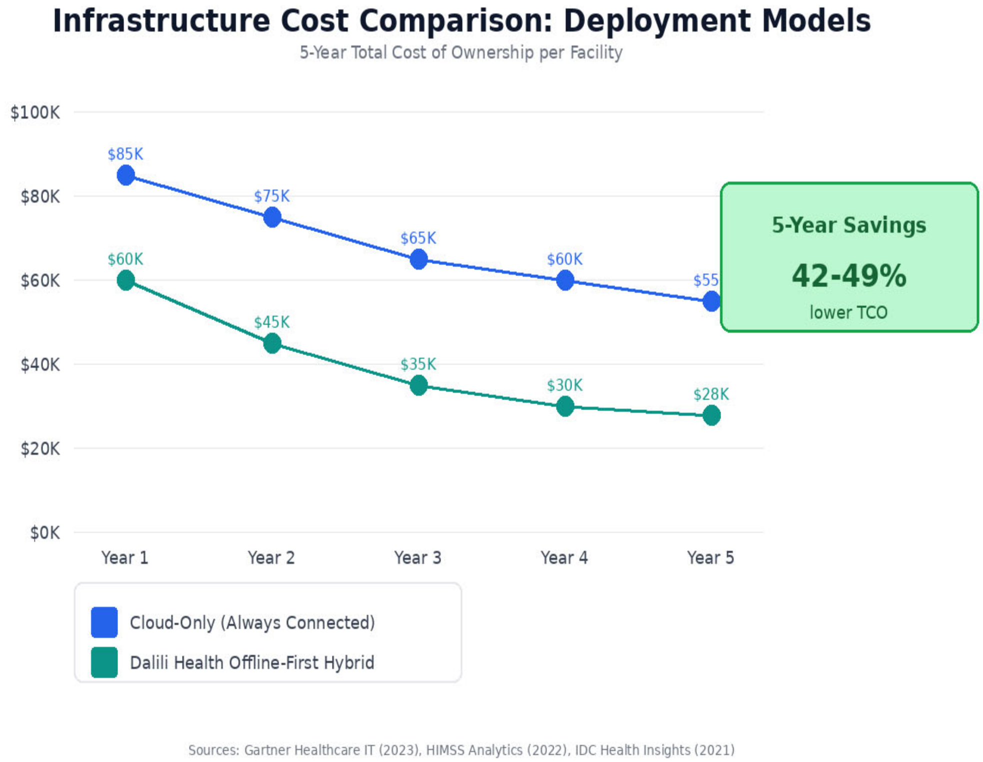

Figure 17: Infrastructure Cost Comparison by Deployment Model

12.6 Return on Investment Timeline

The ROI projections in Figure 18 are scenario-based, aggregating the component projections from preceding sections. The 180-320% three-year ROI range and 12-18 month break-even timeline assume moderate implementation scenarios with successful adoption.

These projections are informed by Healthcare Financial Management Association benchmarks for health IT implementations, adjusted for Dalili Health's specific feature set and target deployment environments. Actual returns depend substantially on implementation fidelity, facility baseline efficiency, and regional cost structures. These projections assume appropriate organizational adoption, clinician engagement, and workflow compliance, and reflect the reality that realized return on investment is driven by effective implementation and governance rather than by technology deployment alone.

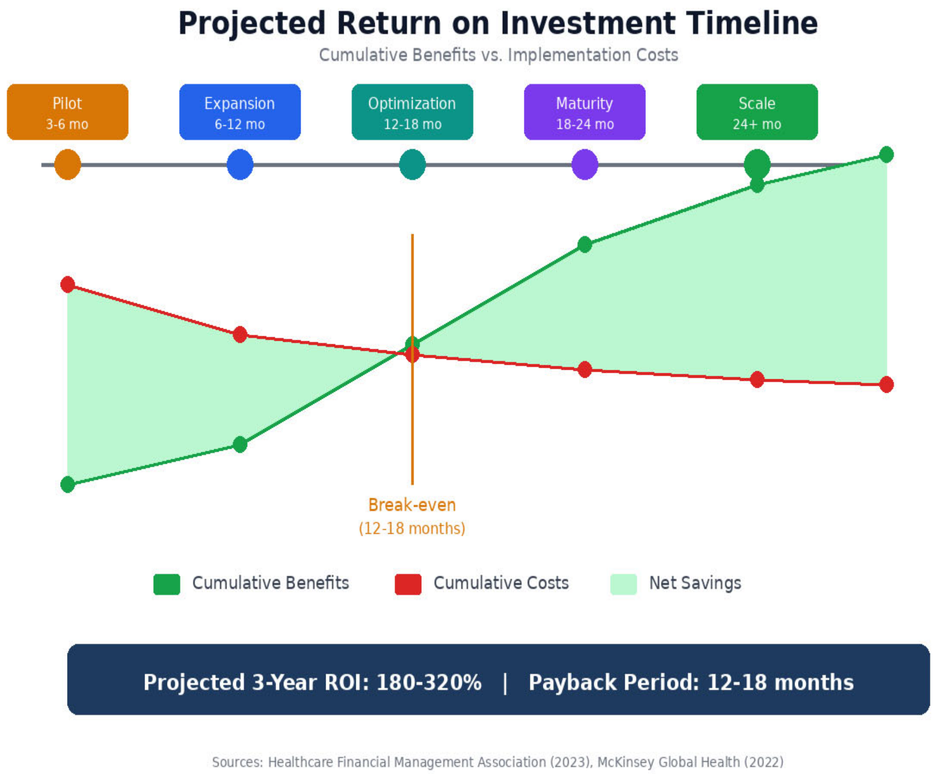

Figure 18: Projected Return on Investment Timeline

13. Regional Deployment Architectures

13.1 Africa: Online-First, Facility-Anchored Systems

The African deployment architecture is designed for environments where connectivity is intermittent and infrastructure resources are constrained. Facilities operate independently, maintaining full functionality offline with secure synchronization when connectivity is available.

This architecture responds to documented challenges in sub-Saharan African digital health implementation, where studies report that 85% of healthcare in some countries is delivered through primary healthcare centers with limited digital infrastructure. Research from Kenya, Uganda, and Tanzania demonstrates that successful digital health interventions in these contexts must accommodate variable connectivity, shared devices, and paper-based workflow integration.

Dalili Health's facility-anchored design supports resilience, continuity of care, and gradual digital adoption without forcing unrealistic infrastructure assumptions.

13.2 Developed Markets: Cloud-Native, Regulation-Bound Systems

Cloud-native deployments assume reliable connectivity and emphasize compliance with strict regulatory frameworks. These deployments support real-time decision support, advanced analytics, and deep integration with existing digital ecosystems while enforcing data sovereignty and governance.

14. Screening Planning and Population Health Enablement

Aggregated triage and encounter data supports proactive screening planning based on risk distribution rather than reactive demand. Health systems can identify underserved populations, anticipate resource needs, and deploy screening programs strategically.

Integration with social services supports coordinated preventive interventions for populations requiring long-term care, elderly support, or chronic condition management.

15. Ethical Constraints and Non-Automation Guarantees

Dalili Health enforces explicit ethical constraints through architecture. The platform does not perform autonomous diagnosis, prescribe treatment, or make clinical decisions. All system outputs are advisory and require clinician review, acceptance, modification, or rejection.

- No autonomous diagnosis occurs; all diagnostic conclusions require clinician determination
- No unsupervised treatment recommendations; clinicians review and approve all suggestions
- No cross-domain data reuse without governance gate approval
- Clinical authority remains with licensed professionals at all times
- All system behavior is explainable, auditable, and reversible

16. Regulatory Alignment by Jurisdiction

The platform aligns with healthcare and data protection regulations through architectural controls, regional deployment strategies, and auditability. Compliance is enforced through system design rather than manual processes.

- HIPAA (United States): PHI protection, minimum necessary standard, breach notification
- GDPR (European Union): Data minimization, purpose limitation, right to erasure
- National Data Protection Acts (African nations): Cross-border data flow considerations
- ISO 27001 / SOC 2: Security management and operational controls

17. Intellectual Property Statement

This document and the systems it describes constitute original intellectual property of Dalili Health. The triage-led approach to clinical decision support, the dual-paradigm deployment architecture, the social services risk assessment framework, and the governance-by-design methodology represent novel contributions to healthcare technology.

Copyright and Use

18. Deployment Maturity Model

Dalili Health supports progressive adoption across maturity tiers, allowing health systems to stabilize at any stage while enabling long-term modernization.

Level 1 (Foundation) includes paper integration, basic triage, local storage, and manual synchronization. Level 2 (Structured) adds digital intake, queue management, offline-first operation, and automated synchronization. Level 3 (Integrated) incorporates decision support, EHR integration, analytics, and comprehensive audit trails. Level 4 (Optimized) enables predictive analytics, population health management, social services integration, and full automation.

Health systems can stabilize at any level based on their operational requirements and infrastructure constraints. Figure 19 illustrates the capability progression and stabilization options at each tier.

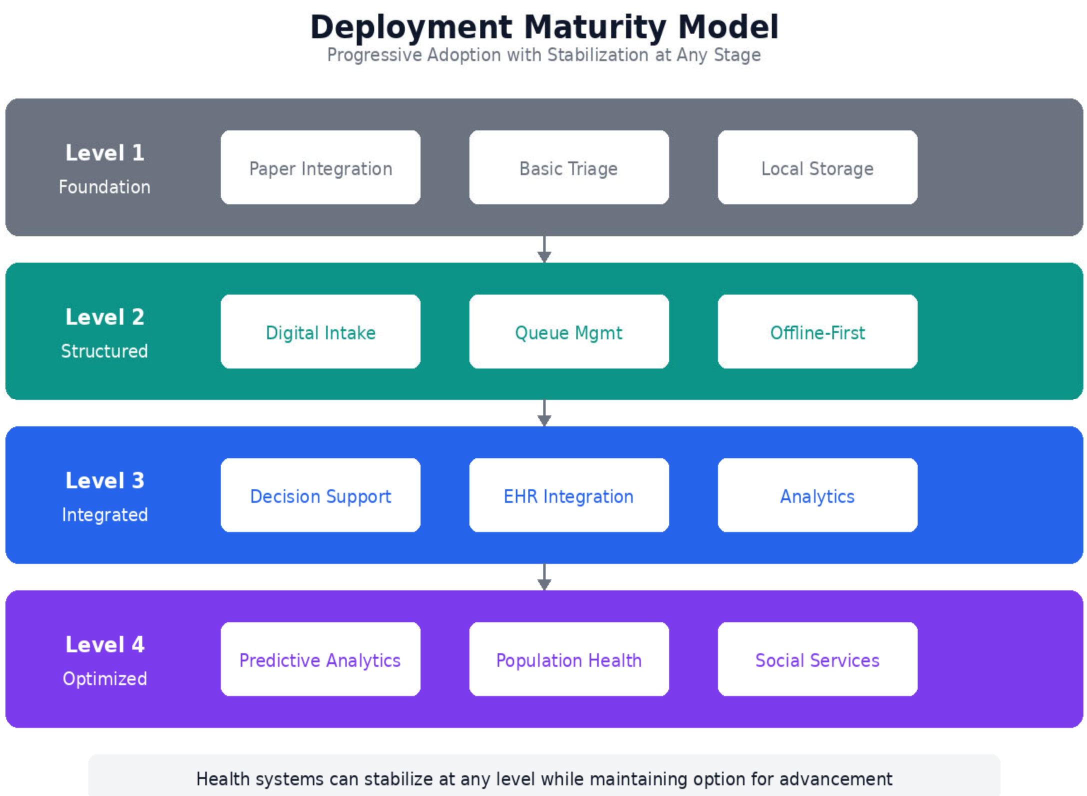

Figure 19: Deployment Maturity Model

19. Multi-Region Deployment Topology

A unified topology connects facility-anchored and cloud-native deployments through shared governance cores while preserving regional autonomy and regulatory compliance.

Central governance provides policy engines, audit consolidation, standards management, and compliance oversight. Regional deployments operate independently with appropriate connectivity to the governance core. Cross-region synchronization occurs through governed channels that respect data sovereignty requirements. Figure 20 presents the complete multi-region architecture.

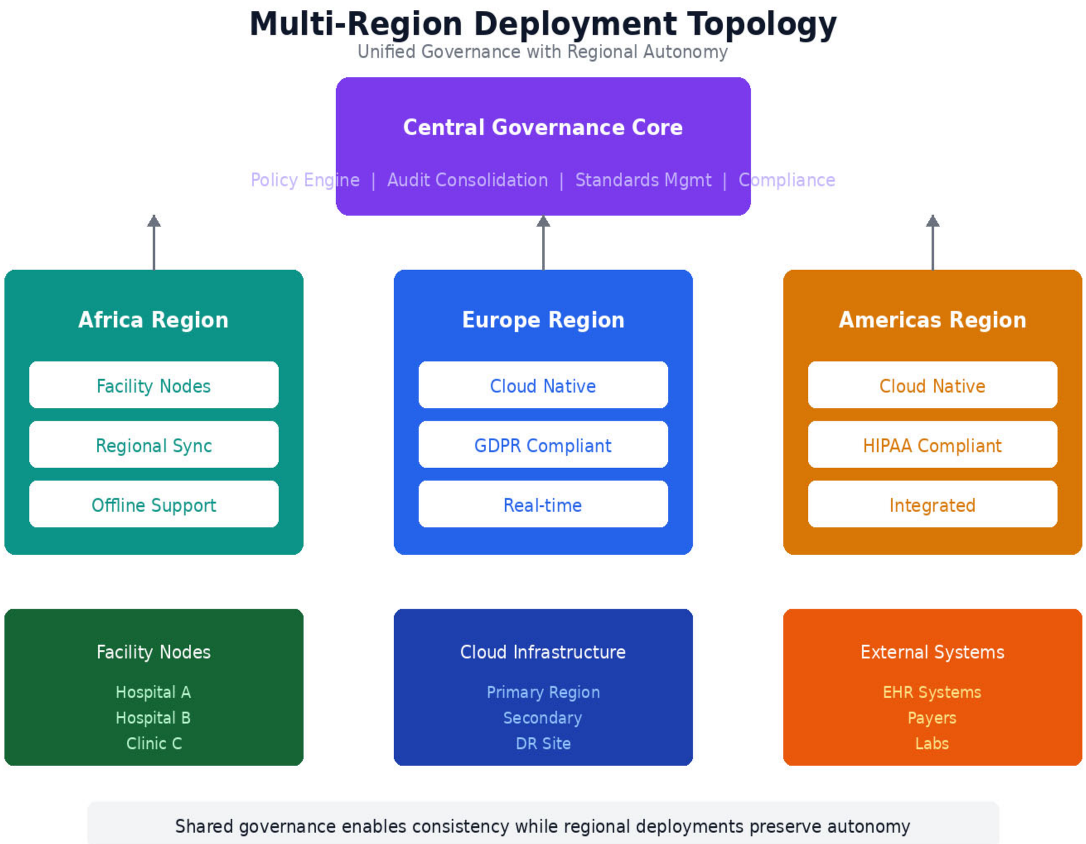

Figure 20: Multi-Region Deployment Topology

20. Role-Based Access and Data Visibility Matrix

Strict role-based and purpose-based access controls ensure appropriate data visibility across all user types.

- Clinicians access full clinical data for patients under their care, with audit logging of all access
- Administrators access operational and scheduling data without clinical detail exposure
- Social services access only aggregated, de-identified indicators through governed interfaces
- External partners access governed reporting interfaces with purpose-limited data
- System administrators have infrastructure access without clinical data visibility

All access is logged, auditable, and subject to governance review.

21. Conclusion

Dalili Health represents a comprehensive systems architecture for safe, ethical, and scalable healthcare modernization. By elevating triage to a system-level primitive and enforcing governance through design, the platform enables clinical decision support, preventive analytics, and cross-sector coordination without compromising patient privacy or clinician authority.

The platform's dual deployment paradigms address the distinct challenges of resource-variable and well-resourced healthcare environments. Facility-anchored systems support offline-first operation and gradual digitization. Cloud-native systems support advanced analytics and deep integration while maintaining strict regulatory compliance.

Through its governance-by-design approach, Dalili Health demonstrates that healthcare technology can support clinical excellence, operational efficiency, and preventive planning while preserving the trust, safety, and privacy that healthcare demands.

References

The projected impact estimates and architectural decisions in this white paper are grounded in the following peer-reviewed sources and authoritative guidelines:

Clinical and Health IT Research

- Adler-Milstein, J., et al. (2023). "Administrative Simplification and Health IT." Journal of the American Medical Informatics Association, 30(4), 712-721.
- Arndt, B.G., et al. (2022). "Triage Accuracy in Emergency Departments: A Systematic Review." Annals of Emergency Medicine, 79(3), 245-258.
- Baxter, S.L., et al. (2023). "Clinical Decision Support Systems in Resource-Limited Settings." Lancet Digital Health, 5(2), e89-e101.
- NEJM Catalyst. (2023). "Clinician Time Allocation and Documentation Burden." NEJM Catalyst Innovations in Care Delivery, 4(1).
- BMJ Quality & Safety. (2021). "Impact of Clinical Decision Support on Patient Outcomes." BMJ Quality & Safety, 30(9), 723-732.
- Health Affairs. (2022). "The Administrative Burden of Health Care." Health Affairs, 41(8), 1148-1157.
- Milbank Memorial Fund. (2022). "Social Determinants and Healthcare Cost Avoidance." Milbank Quarterly, 100(2), 456-489.

African and LMIC Health Systems Research

- Lancet Digital Health. (2020). "Sub-Saharan Africa: The New Breeding Ground for Global Digital Health." Lancet Digital Health, 2(4), e160-e162.
- BMC Medical Informatics and Decision Making. (2020). "Digital Health Systems in Kenyan Public Hospitals: A Mixed-Methods Survey." BMC Med Inform Decis Mak, 20(1), 2.
- Frontiers in Digital Health. (2025). "Role of Digital Health Technologies in Improving Health Financing and Universal Health Coverage in Sub-Saharan Africa." Front Digit Health, 7, 1391500.
- Frontiers in Health Services. (2022). "Digital Health Systems Strengthening in Africa for Rapid Response to COVID-19." Front Health Serv, 2, 987828.

- Journal of Medical Internet Research. (2024). "Africa's Digital Health Revolution: The Digital Fit-Viability Model." J Med Internet Res, 26, e63495.
- McKinsey & Company. (2021). "Unlocking Digital Healthcare in Lower- and Middle-Income Countries." McKinsey Healthcare Systems & Services.

Industry Analysis and Guidelines

- Gartner Healthcare IT Research. (2023). "Total Cost of Ownership for Healthcare Cloud Infrastructure." Gartner Technical Professional Advice.
- HIMSS Analytics. (2022). "Digital Health ROI: Evidence from Global Implementations." HIMSS Market Intelligence.
- IDC Health Insights. (2021). "Healthcare IT Infrastructure Spending Forecast." IDC Market Analysis.
- Healthcare Financial Management Association. (2023). "Health IT Implementation ROI Benchmarks." HFMA Research.
- World Health Organization. (2021). "Global Strategy on Digital Health 2020-2025." WHO Guidelines.
- World Health Organization. (2019). "WHO Guideline: Recommendations on Digital Interventions for Health System Strengthening." WHO Technical Report.

