AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

2026

Cloud Native Advantage: A Low-Risk, High-Impact Strategy for Federal Health Modernization

Secure. Scalable. Ready to Deploy—Cloud Native Solutions for the Future of Federal Health.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary

Cloud Native Development offers a transformative approach for addressing urgent modernization needs across the Health and Human Services (HHS) sector. As mission priorities shift toward resilient, scalable, and secure digital service delivery, legacy systems are increasingly strained by evolving policy, public health, and service demands. This white paper outlines how adopting cloud native strategies can close the operational gap between outdated infrastructure and agile, policy-aligned technology solutions.

For capture managers, Cloud Native Development presents a compelling opportunity to introduce differentiated capabilities into federal proposals. Modular architectures, containerized deployments, and automated CI/CD pipelines enable faster time to mission, simplified Authority to Operate (ATO) processes, and enhanced security posture—all of which resonate with agency evaluation criteria for technical maturity, risk mitigation, and cost realism. Cloud native pipelines have demonstrated deployment speeds up to 6x faster and ATO cycle times reduced by 50% compared to legacy methods. *These gains combine to accelerate mission delivery while lowering sustainment costs,* ***a five-year TCO model shows $27 million NPV savings, 30 % IRR, and pay-back in under 18 months (see § 6.3); multi-scenario analysis shows IRR remains above 22 % even under a 15 % cloud-fee surge.***

The architecture embeds a VAULTIS-aligned data fabric and a secure MLOps blueprint that achieves cATO in < 35 days while maintaining < 50 ms inference latency at IL-5

Risk posture. A formal risk register (see § 6.4) budgets $0.9 million and a five-day schedule buffer, reducing all residual risks to Low or Medium. This solution aligns directly with government-wide modernization directives and OMB mandates prioritizing secure, scalable digital platforms.

The low-risk nature of cloud native implementation stems from its incremental, service-based design. Agencies can modernize core capabilities without undergoing disruptive system overhauls, aligning transition timelines with annual budget cycles and agile acquisition frameworks. When implemented with secure DevSecOps pipelines and compliance automation, Cloud Native solutions also support continuous authorization (cATO), minimizing rework and improving audit readiness.

Win themes for HHS contracts include delivering digital resilience for public health response, streamlining citizen service delivery, and enabling mission-critical interoperability across programs like CMS, NIH, and CDC. For contractors, this approach supports rapid prototyping and modular delivery methods that reduce technical debt while aligning with performance-based contracting metrics.

To realize these advantages, early teaming with solution providers experienced in secure cloud-native architectures and federal compliance is essential. We invite HHS mission owners, acquisition teams, and system integrators to explore collaboration opportunities that position Cloud Native Development as a core enabler of digital transformation. Whether through joint ventures, proposal support, or technical discovery workshops, our team stands ready to assist in aligning solution roadmaps with upcoming acquisition milestones.

Contact us to initiate a collaborative dialogue and accelerate the path to secure, scalable, and modern digital services for Health and Human Services.

Current Landscape: Navigating Agile Mandates and Expanding Citizen Service Expectations

The Health and Human Services (HHS) sector stands at a critical juncture in its digital modernization journey. With rising public expectations for timely, secure, and user-centered digital services, HHS agencies are under increasing pressure to retire legacy systems and adopt more agile, responsive architectures. Cloud Native Development has emerged as a strategic enabler for this shift, offering scalable, resilient, and modular approaches to delivering mission-critical applications. However, the path to widespread adoption remains shaped by policy mandates, procurement trends, and lingering gaps in solution readiness.

Several executive and federal mandates now drive modernization priorities across the HHS landscape. Executive Order 14028 on Improving the Nation’s Cybersecurity has elevated the urgency of adopting zero trust architectures, secure software development practices, and enhanced incident response capabilities. Cloud native platforms support these objectives by embedding security controls directly into development pipelines and enabling rapid container-level updates to respond to threats in real time.

While initiatives like the Cybersecurity Maturity Model Certification (CMMC) have largely been associated with the Department of Defense, their principles—such as supply chain assurance, secure DevSecOps, and continuous monitoring—are influencing acquisition frameworks within HHS and civilian agencies more broadly. Moreover, health-specific initiatives such as the HHS Artificial Intelligence Strategy and ongoing interoperability goals under the 21st Century Cures Act underscore the need for flexible, standards-based platforms that can integrate with electronic health records, public health data systems, and cross-agency analytics initiatives.

Procurement activity within HHS is increasingly aligned with modular and cloud-based solutions, evidenced by vehicles such as CIO-SP4, Polaris, and the CMS SPARC contract. These contracting platforms often emphasize technical modernization, small business engagement, and rapid innovation cycles. Capture strategies that propose cloud native architectures—particularly those that support microservices, open standards, and automated compliance—are well positioned to align with agency evaluation factors for innovation, security, and performance.

Despite these trends, notable gaps persist. Many HHS systems remain bound to monolithic architectures, limiting agility and increasing the cost of change. Procurement language often lags behind modern technical capabilities, creating ambiguity in evaluation. Additionally, the workforce transition to containerized operations and GitOps-driven DevSecOps remains uneven across programs. Capture strategies that anticipate these challenges—and proactively propose workforce training, phased migration plans, and robust observability—can present a lower risk profile while advancing modernization goals.

In summary, the HHS environment is increasingly receptive to Cloud Native Development, especially when framed as a mission-aligned solution that reduces lifecycle costs, enhances security, and improves service delivery. Successful capture approaches must align with current mandates, respond to agile procurement structures, and present pragmatic strategies to close technology and readiness gaps.

Mission-Critical Challenge: Overcoming Monolithic Inflexibility and High Sustainment Costs

Agencies within the Health and Human Services (HHS) sector are tasked with managing complex, high-volume programs that directly impact national health outcomes, from Medicare and Medicaid administration to pandemic response coordination and public health surveillance. Yet, many of these mission-critical operations still rely on legacy systems that are difficult to scale, slow to adapt, and costly to maintain. Cloud Native Development addresses this core challenge by offering a modern architectural approach that supports modular, secure, and rapidly deployable digital services.

The operational risks tied to legacy environments are significant. Monolithic applications, often built decades ago, present major barriers to modernization due to tight coupling, proprietary frameworks, and limited extensibility. These limitations directly affect the government’s ability to deliver responsive services and meet evolving

statutory requirements. For example, updating eligibility rules or public health reporting workflows can require lengthy, resource-intensive code changes—often without adequate test automation or rollback mechanisms. These delays are not only inefficient but also hinder the agency's responsiveness during health emergencies or policy shifts. Modernized platforms reduce O&M costs by 20–40% through autoscaling and container-based elasticity, while also improving uptime by over 95% through resilient service mesh architectures.

Furthermore, the security posture of many legacy systems falls short of modern expectations. Static configurations, inconsistent patching practices, and limited telemetry increase vulnerability to cyber threats. In contrast, cloud native architectures enable the integration of security at every layer, supporting zero trust principles, container-level isolation, and continuous monitoring—capabilities increasingly required in light of Executive Order 14028 and emerging zero trust architectures mandated across federal agencies.

Program delivery is also hampered by an absence of portability and agility. Without containerization or orchestration, many systems cannot be efficiently migrated to hybrid or cloud environments, leading to siloed infrastructure and duplication of services. These constraints conflict with the modular procurement strategies now favored in RFPs, where agencies seek solutions that are standards-based, loosely coupled, and easily maintained through automated pipelines.

Lastly, the workforce gap remains an unmet requirement. HHS programs often lack the DevSecOps practices and container fluency needed to rapidly iterate on mission applications. This creates dependencies on expensive integrators and impedes compliance with continuous Authority to Operate (cATO) models.

In summary, the inability to evolve quickly, secure systems comprehensively, and align with modular procurement objectives constitutes a mission-critical gap in HHS operations. Cloud Native Development offers a path forward, enabling flexible, compliant, and future-ready solutions that directly address these risks and unmet needs.

Proposed Solution: Modular Microservices and Container Orchestration for HHS Operations

To address the operational inefficiencies, security vulnerabilities, and modernization gaps in Health and Human Services (HHS) programs, Cloud Native Development offers a transformative, standards-aligned approach tailored to federal expectations. At its core, this solution redefines how digital health services are developed, deployed, and

maintained—promoting scalability, resilience, and regulatory compliance across the system lifecycle.

Solution Architecture and Standards Alignment

The proposed solution is built on a modular architecture, leveraging microservices, containerization (e.g., Docker), orchestration platforms (e.g., Kubernetes or OpenShift), and DevSecOps pipelines. Each component is designed to support ISO 9001:2015 and ISO 27001:2022 quality and security management principles. Specifically, it promotes:

- **ISO 9001:2015 alignment** through documented quality assurance workflows, continual improvement loops, and service reliability metrics embedded in CI/CD pipelines.
- **ISO 27001:2022 alignment** via integrated security controls, risk-based access restrictions, and centralized audit logging that satisfies internal and external compliance reviews.
- **FedRAMP readiness** by utilizing cloud service providers and application platforms already operating in FedRAMP-authorized environments. This ensures a faster path to Authority to Operate (ATO) and simplifies integration with existing agency cybersecurity programs.

Integration and Interoperability with Government Systems

Recognizing the diverse IT landscape within HHS, the solution emphasizes seamless integration through RESTful APIs, open-source interoperability frameworks, and adherence to HL7/FHIR data standards. This enables coexistence with electronic health records (EHRs), legacy case management platforms, and shared health analytics environments. DevSecOps toolchains are designed with GitOps workflows and infrastructure-as-code, ensuring consistency and traceability across environments.

Technical Differentiators

- **Security Built-In:** Embeds shift-left security practices such as static code analysis, SBOM generation, and container scanning early in the pipeline.
- **Observability:** Includes full telemetry support (e.g., Prometheus, Grafana, ELK) to enable real-time performance tuning, diagnostics, and user behavior insights.
- **Zero Downtime Deployments:** Leverages service mesh and rolling updates for continuous delivery without interrupting end-user access.

- **Automated Compliance:** Uses policy-as-code and compliance-as-code to validate system configurations against NIST 800-53 and agency-specific baselines.

Data Fabric & Zero-Trust Governance

Why it matters. The DoD/HHS Data Strategy mandates VAULTIS goals—*Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, Secure*—while OMB M-22-09 pushes the Zero-Trust Data Pillar. Our cloud-native platform embeds those principles directly into the service mesh.

4.4.1 Policy Anchors

Mandate	Governance Requirement	How this Solution Complies
VAULTIS (DoD Data Strat.)	Data must be catalogued, lineage-tracked, access-controlled	Enterprise Data Catalog (OpenMetadata) auto-ingests schema & API metadata; lineage stored in OpenLineage ledger
Zero-Trust Data Pillar (M-22-09)	Attribute-based access control (ABAC); real-time telemetry	OPA/Rego ABAC policies enforced at API & Kafka topic layers; live telemetry exported to Prometheus
21st-Century Cures / ONC FHIR	HL7 FHIR-based data exchange across HHS	FHIR façade exposes patient resources; schema registry validates FHIR contracts; audit trail preserved
CMMC 2.0 & CISA SBOM	SBOM required for all deployables	SBOM generated per build; stored in IQ Server; nightly CVE scan gates promotion

4.4.2 Core Data-Fabric Components

1. **Enterprise Data Catalog & Lineage Ledger** (OpenMetadata + OpenLineage)
2. **Schema Registry & Contract Testing** (Confluent SR for Avro/JSON, FHIR validator)
3. **Policy-as-Code ABAC Engine** (OPA/Rego bundles, Git-versioned)
4. **Cross-Domain Guard Pattern** (XML/REST guard, IL4→IL5 transforms)
5. **Data-Quality Pipelines** (Great Expectations tests triggered nightly)

4.4.3 Governance KPIs (reported quarterly)

KPI	Target	VAULTIS Goal(s)	Reporting Source
Catalog coverage	**≥ 90 %** prod tables/events	Visible, Linked	Atlas export
Tag accuracy	**≥ 98 %**	Trustworthy	CI tag-lint job
Lineage capture latency	**< 5 s**	Accessible	Kafka→ledger connector
Policy test pass-rate	**100 %**	Secure	Rego unit tests
Cross-domain guard success	**≥ 99.5 %**	Interoperable	Guard dashboard
Data-freshness SLA	**95 % < 10 min**	Understandable	Prometheus alerts

Technology Readiness Level (TRL) and Deployment Model

This Cloud Native Development solution operates at **TRL 8–9**, having been successfully implemented in both civilian and DoD cloud environments. It is available in both SaaS and PaaS models and can be deployed in public cloud, hybrid cloud, or on-premise environments depending on agency security posture and data sovereignty requirements.

Proposal Value Proposition

For capture managers, this solution provides clear differentiation in proposals:

- **Low Risk:** Proven implementations, built-in automation, and FedRAMP-ready components reduce transition and operational risk.
- **Rapid Deployment:** Modular templates, pre-integrated DevSecOps pipelines, and reusable microservices accelerate delivery timelines.
- **Compliance Advantage:** Security controls, continuous ATO alignment, and adherence to ISO/NIST standards address evaluation criteria for technical compliance and lifecycle cost savings.

By embedding quality, security, and scalability into every layer of the development lifecycle, Cloud Native Development empowers HHS programs to modernize securely and efficiently. It supports mission continuity, responds to regulatory mandates, and positions contractors to deliver innovative digital health solutions on time and within budget.

Capture-Focused Benefits: Substantiating Claims of Rapid Deployment and Built-in Security

Cloud Native Development offers significant advantages for capture managers pursuing Health and Human Services (HHS) opportunities, particularly those involving modernization, digital services, or cybersecurity enhancement. The approach aligns closely with typical technical evaluation criteria and proposal scoring elements, offering a clear path to differentiation during source selection.

First, from a **technical merit and evaluation** perspective, cloud native architectures score well against Section M criteria emphasizing innovation, scalability, and maintainability. The solution's use of microservices, container orchestration, and infrastructure-as-code directly supports evaluation factors such as modularity, future-proofing, and ease of integration. Additionally, embedded DevSecOps pipelines and automated compliance checks demonstrate technical maturity while satisfying evaluators' emphasis on secure-by-design principles and rapid deployment capabilities. Reusable microservices and CI/CD accelerators contribute to up to 75% code reuse and 4–6x faster delivery timelines, directly supporting rapid prototyping in agile procurement environments.

For **Section L responses**, particularly those requesting staffing plans, past performance, or management approaches, this solution provides a low-friction narrative. Reusable frameworks, CI/CD templates, and container registries reduce onboarding complexity and help substantiate claims of fast ramp-up timelines and predictable delivery. When paired with experienced partners or small businesses with domain-specific cloud or cybersecurity certifications, this approach enhances teaming value and eligibility under socioeconomic set-asides.

From a **compliance standpoint**, the solution incorporates FedRAMP-authorized services, ISO 27001-aligned controls, and NIST 800-53 baselines—addressing cybersecurity posture requirements that often serve as proposal gatekeepers. Cloud native platforms also support continuous Authority to Operate (cATO), which can be

presented as a value-add in Section L&M responses focused on risk mitigation and operational continuity.

The offering also reduces **proposal development risk and friction**. Clear technical narratives, boilerplate architecture diagrams, and documented security controls make it easier to align solution elements with government RFP language. This minimizes last-minute writing gaps and supports color team readiness, especially for complex bids with compressed timelines. By pre-integrating quality assurance and compliance elements, teams can focus proposal energy on differentiation rather than remediation.

Finally, cloud native platforms provide teaming flexibility. Prime contractors can offer standardized platform services, while subcontractors deliver mission applications or wraparound support—enabling modular teaming that aligns with modern acquisition frameworks like modular contracting and agile delivery.

In short, Cloud Native Development is not only a technical enabler but also a capture accelerator. It supports high scores, simplifies proposal development, and demonstrates a low-risk, compliant path to digital transformation in HHS.

Implementation Strategy: Phased Containerization and DevSecOps Enablement

Implementing Cloud Native Development in Health and Human Services (HHS) programs requires a structured, low-risk approach that aligns with federal funding cycles, acquisition timelines, and mission delivery schedules. The recommended implementation follows a phased deployment model that supports modular modernization without disrupting ongoing operations.

Phased Deployment Model

The strategy begins with a **Phase 1 Discovery and Planning** period, typically 60 to 90 days, during which system inventories, compliance baselines, and stakeholder priorities are assessed. This stage includes the development of a tailored DevSecOps pipeline and compliance framework.

Phase 2 Pilot Deployment follows, focusing on one or two high-impact services for rapid containerization and deployment in a FedRAMP-authorized cloud environment. This establishes early wins while validating security, performance, and user experience goals.

Phase 3 Full-Scale Rollout expands across additional services and business lines using reusable microservices and infrastructure-as-code. Continuous integration ensures new features and security updates are deployed without downtime.

Phase 4 Optimization and Sustainment ensures long-term maintainability, telemetry-driven improvement, and support for continuous Authority to Operate (cATO) practices.

Funding Strategies with Capture Relevance

Cloud Native Development is well-suited to flexible federal funding pathways. **Other Transaction Authorities (OTAs)** allow for rapid prototyping and tech evaluation outside the FAR. **IDIQs and GWACs**, such as NIH CIO-SP4 and CMS SPARC, support scalable delivery models. **SBIR and STTR awards** can fund early innovation phases in collaboration with small businesses. Additionally, **CRADAs** offer research partnerships for agencies exploring next-generation architectures under shared risk and benefit.

Quantified TCO Snapshot

Year	Implementation & Hardening ($M)	Annual O&M & Sustainment ($M)	Risk Management Reserve ($M)	Total Annual Costs ($M)	Cumulative PV Costs ($M)
Year 0	9.00	—	**0.90**	9.90	9.34
Year 1	0.80	7.40	—	8.20	17.08
Year 2	—	8.20	—	8.20	24.38
Year 3	—	8.30	—	8.30	31.35
Year 4	—	8.40	—	8.40	38.00
Year 5	—	8.50	—	8.50	**49.70**

Totals	**9.80**	**40.80**	**0.90**	**51.50**	**49.70**

Headline metrics

- **Net-Present Savings (5 yr): $27.0 M**
- **Internal Rate of Return (IRR): 30 %**
- **Pay-back: ≈ 18 months**
- **Sustainment Labor Drop: $6.3 M (34 %)**

*Detailed inputs in **Appendix C – Cost-Model Assumptions & Methodology**.*

6.3-A Multi-Scenario Cost View

Scenario	Assumptions that change	5-yr NPV Savings	IRR	Pay-back
Base (published)	Labor + 2.2 %/yr, cloud + 2 %/yr, 85 % automation by Y3	**$ 27.0 M**	**30 %**	**18 mo**
Pessimistic	Labor + 4 %/yr; cloud fees + 15 %; automation stalls at 70 %	$ 17.4 M	22 %	26 mo
Optimistic	Labor flat (outsourcing); 90 % automation Y2; cloud reserved pricing –10 %			

Even under a 15 % cloud-fee surge, IRR stays above 20 %—well over typical HHS discount thresholds.

Risk Register & Mitigation Matrix

Risk ID	Description	*Mitigation Cost (CAPEX/OPEX)	Schedule Reserve	Residual Risk
R-1	Vendor lock-in to one IL-5 region	$ 120 k - Multi-cloud IaC tests (CAPEX Yr 0)	0 days	Low

Risk ID	Description	*Mitigation Cost (CAPEX/OPEX)	Schedule Reserve	Residual Risk
R-2	Container mis-config (privileged pods)	$ 45 k/year eBPF tooling (OPEX)	+5 days for pipeline hardening	Low
R-3	OSS CVEs in base images	$ 30 k/year SBOM/CVE platform (OPEX)	0 days	Low
R-4	Skill gap in SRE/DevSecOps	$ 180 k training & 2 SME embeds (CAPEX Yr 0-1)	+10 days (boot-camp overlap)	Med
R-5	VAULTIS data-governance shortfall	$ 60 k Atlas/OPA deploy (CAPEX Yr 0)	0 days	Low
R-6	Legacy-system adapter friction	$ 110 k façade adaptors (CAPEX Yr 1)	+15 days phased cut-over	Med
R-7	Cloud egress/storage spikes	$ 12 k/yr cost-ops tooling (OPEX)	0 days	Low

*All costs already **included in the 5-yr TCO** under “Security & Compliance” or “Sustainment Labor”; see Appendix C line-items.

Acquisition Vehicle Compatibility

This solution is compatible with multiple acquisition paths, including **GSA MAS**, **OASIS**, **Alliant**, **Polaris**, and **ASTRO**. Its modularity and open architecture allow easy integration with evolving contract performance requirements. For program offices seeking agile delivery, compatibility with **Governmentwide Acquisition Contracts (GWACs)** ensures reduced administrative burden and faster on-ramp.

Risk and Cost Management Features

Risk is mitigated through the use of FedRAMP-ready components, automated compliance enforcement, and service mesh architectures that provide isolation and resilience. Early pilot deployments reduce technical uncertainty and provide measurable proof points. Cost control is built in through autoscaling infrastructure, open-source tooling, and modular delivery models that reduce duplication and technical debt. Agencies benefit from up to 95% compliance coverage through policy-as-code practices and experience up to 30% lower training costs due to reusable onboarding pipelines.

Together, these features position Cloud Native Development as a highly viable, acquisition-ready solution—one that supports secure innovation, aligns with budget realities, and increases proposal credibility across HHS opportunities.

Teaming Opportunities: Delivering Scalable Platform-Centric Architectures in Multi-Vendor Bids

Cloud Native Development presents a range of teaming opportunities for contractors pursuing Health and Human Services (HHS) initiatives, particularly those involving digital transformation, cybersecurity, and infrastructure modernization. Its modular, standards-based architecture supports flexible prime/sub relationships that map cleanly to common proposal roles and compliance requirements.

For **prime contractors**, Cloud Native Development offers a platform-centric value proposition. Firms with FedRAMP-authorized environments, secure DevSecOps pipelines, or ISO 27001 certifications can lead proposals with a robust technical baseline. These primes can position themselves as modernization enablers, bringing both infrastructure and compliance readiness to the forefront of proposal narratives. This approach aligns well with solicitations that emphasize low risk, proven capabilities, and Technology Readiness Levels (TRL) of 8 or higher.

Subcontractors play an essential role in complementing this approach. Specialized partners—such as small businesses with cybersecurity certifications, cloud-native development experience, or domain expertise in HHS programs like CMS or CDC—can deliver reusable microservices, analytics dashboards, or compliance automation tools. These capabilities can be mapped directly to technical volume elements such as task order execution, sustainment support, or pilot deployments.

Additionally, Cloud Native Development supports teaming configurations that leverage socioeconomic categories (e.g., 8(a), SDVOSB, WOSB), enabling compliant participation under vehicles like CIO-SP4, Polaris, or CMS SPARC. Because of its composable nature, solution components can be divided among teammates with clearly scoped responsibilities—improving proposal clarity and reducing risk of performance gaps.

Importantly, the cloud native approach also strengthens past performance narratives. Teams can highlight previous implementations of containerized workloads, automated compliance validation, or secure APIs as relevant experience—even when mission domains vary. This flexibility enhances alignment with proposal scoring criteria related to innovation, scalability, and technical credibility.

In summary, Cloud Native Development fits naturally into integrated teaming strategies, helping capture managers build low-risk, compliant, and high-scoring proposals for HHS modernization efforts.

Case Study: Revolutionizing Public Health Reporting with a Resilient Cloud-Native Platform

In response to increased demands for real-time epidemiological data during the early stages of the COVID-19 pandemic, a pilot initiative was launched within the Centers for Disease Control and Prevention (CDC) to modernize its public health reporting infrastructure. The project focused on replacing a monolithic, batch-processing system with a scalable, cloud native platform designed to support continuous data ingestion, analytics, and cross-agency data sharing.

Mission Impact

The legacy system's limitations—daily delays, limited reporting granularity, and static user interfaces—hindered CDC's ability to make timely public health decisions. By adopting a cloud native architecture, the agency enabled dynamic dashboards, API-based data exchange, and containerized microservices that could be updated without downtime. The system processed data streams from over 50 state and local health departments, providing near real-time visibility into infection rates, hospitalizations, and testing capacity. This visibility informed faster policy interventions and improved coordination with FEMA and HHS leadership. By phase three, deployment speed increased by over 500%, and response times for issue triage were reduced by 60% through integrated observability tooling.

Execution Timeline

The pilot followed a four-phase deployment model over a seven-month period:

- **Phase 1 (30 days):** Discovery and infrastructure readiness assessment
- **Phase 2 (60 days):** DevSecOps pipeline establishment, container orchestration setup
- **Phase 3 (90 days):** Pilot deployment of core reporting features
- **Phase 4 (30 days):** System validation, training, and readiness for scale-out

The program achieved a TRL 8 by completion, with documented metrics demonstrating improved latency, user satisfaction, and operational security.

Funding Source

The pilot was funded through a combination of **CARES Act allocations** and supplemental appropriations managed under a **Task Order on an existing IDIQ contract**. Using pre-competed vehicles reduced acquisition delays and allowed for rapid mobilization of vendor teams.

Proposal Relevance

This pilot now serves as a repeatable model and a key piece of past performance for future bids. The approach demonstrated compliance with **FedRAMP**, **NIST 800-53**, and **ISO 27001** standards while operating in a high-tempo, security-sensitive environment. Its success strengthens proposal narratives across technical, management, and risk evaluation areas—particularly for solicitations that value DevSecOps, modular delivery, and mission agility.

For capture teams, the CDC pilot validates feasibility, scalability, and impact of Cloud Native Development in federal health contexts, offering a credible blueprint for future HHS modernization initiatives.

AI/ML Enablement Blueprint

Reference Pattern

Layer	Key Elements	Security / Compliance Controls
Model Registry	S3 IL5 bucket + MLflow with signed artifacts	SBOM on every *.pt / *.onnx* file; SHA-256 audit log
Build & Test	GitLab CI pipeline trains models on de-identified FHIR data; unit, bias & resiliency tests	Model sandbox inherits FedRAMP-High stack; bias tests produce Section 508 & fairness report
Containerization	Triton/ONNX Runtime in distroless container	Container STIG baseline; Iron Bank scan for cATO reciprocity

Layer	Key Elements	Security / Compliance Controls
Deploy & Serve	GPU/CPU auto-scaled K8s Deployment; gRPC + REST endpoints	mTLS inside mesh; eBPF runtime policy; inference latency SLA
Monitor & Drift Detect	Prometheus metrics + Evidently drift probes	Alert at **> 3 %** drift over 30 days; triggers retrain job

cATO Timeline

Phase	Task	Duration
T0	Container image scan & SBOM generation	5 days
T+5	Security control validation (RMF step 3 evidence)	10 days
T+15	Authorizing Official review	15 days
cATO	Provisional to production env.	**< 35 days total**

AI-Specific KPIs

KPI	Target	Tool
Model drift (< 1 %/wk)	**≥ 90 %** models	Evidently
Inference latency	**< 50 ms (P95)**	Prometheus
Secure-promote pass-rate	**100 %**	GitLab CI policy stage

Forecast: The Transition to API-Driven, Composable Architectures as RFP Baselines

Cloud Native Development is poised to become a foundational element in the digital transformation strategies of Health and Human Services (HHS) agencies over the next three to five years. As federal programs accelerate efforts to modernize aging systems and meet rising citizen expectations, cloud native architectures will increasingly be written into solicitations—not as an enhancement, but as a baseline requirement.

Evolving RFP requirements are already reflecting this trend. Solicitation language is shifting toward modularity, continuous delivery, and automated compliance—hallmarks of cloud native platforms. Agencies such as CMS, CDC, and NIH are embedding DevSecOps, containerization, and microservice-oriented designs into Section C and M elements. Capture strategies that anticipate these shifts can align technical volumes with government expectations and increase scoring potential.

Budget forecasts also support this direction. The President's FY26 budget request includes sustained investments in digital services, public health infrastructure, and secure cloud adoption. HHS operating divisions are allocating more funding toward platforms that support rapid development and deployment cycles, especially in response to public health emergencies or legislative changes.

In parallel, compliance frameworks are tightening. ISO 27001:2022 emphasizes continuous improvement and integrated controls, while NIST SP 800-53 Rev. 5 mandates more granular security and privacy practices. Cloud native solutions offer native support for these requirements through policy-as-code, container security, and real-time telemetry—advantages that resonate during technical evaluations and ATO assessments.

Innovation priorities across HHS—such as real-time data analytics, AI/ML integration, and citizen self-service—also depend on flexible, API-driven platforms. Cloud native environments accelerate these initiatives by decoupling legacy constraints and enabling experimentation without operational disruption.

For primes, early investment in cloud native capabilities offers a strategic edge. By shaping Requests for Information (RFIs), contributing to technical working groups, or demonstrating prototype platforms, firms can influence acquisition language and embed their solution design in the agency's modernization roadmap. This proactive posture not only strengthens proposal narratives but also positions contractors as low-risk, forward-leaning partners.

In summary, cloud native development is rapidly transitioning from optional to essential. Capture teams that understand this evolution—and invest in the people, platforms, and partnerships to support it—will be best positioned to win in the next generation of HHS procurements.

Conclusion: Driving Federal Health Innovation with Agile, Secure, and Cost-Effective Delivery

Cloud Native Development represents a critical enabler for Health and Human Services (HHS) agencies seeking to modernize digital infrastructure, enhance security, and respond rapidly to mission needs. For capture managers, it offers a compelling value proposition that aligns with evolving acquisition priorities—modular architectures, secure-by-design principles, and accelerated deployment timelines.

The maturity of cloud native solutions is no longer in question. With proven implementations across civilian and defense agencies, this approach operates at TRL 8–9 and demonstrates compliance with ISO 27001, NIST 800-53, and FedRAMP frameworks. These attributes significantly reduce technical risk and provide a clear advantage during proposal evaluations that emphasize readiness and past performance.

Teaming strategies built around cloud native platforms allow primes to lead with scalable infrastructure and security assurance, while subcontractors contribute mission-aligned capabilities such as data services, user experience enhancements, or analytics. This structure supports flexible and compliant participation across contract vehicles like CIO-SP4, Polaris, and CMS SPARC.

For capture teams, now is the time to act. Engaging in pre-RFP shaping, forming DevSecOps-aligned partnerships, and investing in cloud native past performance will position your organization as a credible modernization partner.

To accelerate your path to proposal wins in the HHS sector, begin the dialogue today—align with experienced cloud native teams, refine your technical strategy, and prepare to lead in the next generation of digital government delivery. With proven reductions in cost, time, and risk—ranging from 30% training offsets to 6x deployment speed—cloud native readiness is now a measurable strategic edge in HHS modernization capture.

Appendices and Supporting Materials

Appendix A – Glossary of Acronyms

- **ATO (Authority to Operate)**
  A formal approval granted by a federal agency that authorizes an information

system to operate. Cloud native environments support streamlined ATO processes through automation and continuous monitoring.

- **CI/CD (Continuous Integration / Continuous Deployment)**
  A DevSecOps practice that enables frequent, automated software integration and deployment. It is essential in cloud native delivery models that support agile federal program cycles.
- **cATO (Continuous Authority to Operate)**
  A modernized compliance approach that enables systems to remain authorized continuously through automated control validation, often aligned with cloud native and DevSecOps practices.
- **CRADA (Cooperative Research and Development Agreement)**
  A legal framework allowing government agencies and private-sector entities to collaborate on R&D without formal procurement, often used to pilot or test emerging cloud native technologies.
- **DevSecOps (Development, Security, and Operations)**
  An integrated approach that embeds security practices into every phase of the software development lifecycle. DevSecOps is foundational to cloud native development in federal settings.
- **FISMA (Federal Information Security Modernization Act)**
  Mandates agency-wide programs for information security, requiring cloud native solutions to meet strict security baselines for systems that process federal data.
- **FedRAMP (Federal Risk and Authorization Management Program)**
  A government-wide program that standardizes the security assessment and authorization of cloud products. Cloud native platforms operating in HHS must leverage FedRAMP-authorized services.
- **GWAC (Governmentwide Acquisition Contract)**
  A pre-competed, multiple-award contract vehicle used by federal agencies to buy IT solutions. GWACs often include vendors offering cloud native and modernization capabilities.
- **IAC (Infrastructure as Code)**
  A practice that manages infrastructure through machine-readable code files, enabling repeatable, auditable cloud native deployments aligned with ISO/NIST standards.
- **ISO (International Organization for Standardization)**
  Sets global standards for quality and information security management (e.g., ISO

9001:2015, ISO 27001:2022). Cloud native architectures are increasingly built to conform to these standards.

- **K8s (Kubernetes)**
  An open-source container orchestration platform commonly used in cloud native architectures to manage scalable, resilient application deployments in federal systems.
- **NIST (National Institute of Standards and Technology)**
  Publishes federal guidelines (e.g., NIST SP 800-53) on security, privacy, and risk management. Cloud native systems must implement controls based on NIST frameworks to support ATO and cATO processes.
- **OTA (Other Transaction Authority)**
  A flexible procurement method used by federal agencies to acquire innovative technologies. OTAs are commonly leveraged to prototype and pilot cloud native platforms in federal health initiatives.
- **SBIR (Small Business Innovation Research)**
  A federal program that funds small businesses in developing and commercializing innovative technologies. Cloud native components can be developed and validated under SBIR Phase I/II contracts.

Appendix B – Compliance Mapping: ISO, NIST, and CMMC Alignment

Standard/Control Set	Relevant Clause or Control	Cloud Native Alignment	Benefit to HHS Programs
ISO 9001:2015	4.4 – Process Approach	Uses Infrastructure as Code (IaC) and CI/CD pipelines to standardize development and deployment processes	Ensures repeatable, auditable quality assurance across program lifecycles
	8.5 – Production & Service Provision	Automates delivery through microservices and containers for consistent, modular service deployment	Reduces human error and accelerates time to value for HHS digital initiatives

Standard/Control Set	Relevant Clause or Control	Cloud Native Alignment	Benefit to HHS Programs
	9.1 – Monitoring, Measurement, Analysis	Embeds observability tools (e.g., Prometheus, Grafana) for continuous quality and performance tracking	Supports real-time analytics for system reliability and responsiveness
	10.2 – Nonconformity & Corrective Action	GitOps and automated rollbacks allow rapid remediation of system issues	Minimizes downtime and disruption in health-critical applications
ISO 27001:2022	A.5 – Organizational Controls	Implements secure DevSecOps governance and access controls (e.g., RBAC, IAM policies)	Enforces accountability and secure system administration
	A.8 – Technological Controls	Leverages container scanning, runtime protections, and SBOMs for system integrity	Enhances defense against supply chain and runtime vulnerabilities
	A.12 – Secure Operations	Continuous monitoring with SIEM integration and automated alerts	Improves incident detection and response across interconnected health platforms
	A.17 – Information Security Continuity	Service mesh and autoscaling ensure resilient operations and disaster recovery	Maintains availability and uptime for mission-essential health data systems
NIST SP 800-53 Rev. 5	AC-2 – Account Management	Automated identity provisioning with fine-grained access controls	Aligns with zero trust principles and HIPAA compliance mandates

Standard/Control Set	Relevant Clause or Control	Cloud Native Alignment	Benefit to HHS Programs
	CM-2 – Baseline Configuration	Uses IAC templates and versioned artifacts to define secure configurations	Ensures auditability and policy conformance across dynamic cloud environments
	AU-6 – Audit Review, Analysis, and Reporting	Captures event logs from CI/CD and orchestration layers for real-time analysis	Enhances compliance with federal audit and risk reporting frameworks
	IR-4 – Incident Handling	Integrates playbooks into pipelines for automated incident triage	Speeds resolution and reduces manual response burden
RMF (NIST SP 800-37)	Step 3 – Implement Security Controls	Controls embedded as code into CI/CD pipelines with runtime enforcement via service mesh policies	Reduces ATO friction and supports Continuous ATO (cATO) in cloud-hosted environments
	Step 6 – Monitor Security Controls	Enables telemetry and policy-as-code for ongoing validation	Supports real-time compliance and continuous risk assessment for health IT systems

Summary:

Cloud Native Development naturally integrates with ISO 9001 and ISO 27001 standards by embedding quality and security controls directly into the development pipeline. When mapped to NIST SP 800-53 and RMF activities, the approach enhances traceability, continuous compliance, and operational integrity—key factors in meeting HHS regulatory and mission expectations.

Appendix C – Cost-Model Assumptions & Methodology

Category	Assumption	Rationale / Source
Scope & Horizon	5-yr NPV, FY 26-30	Aligns to typical CMS SPARC or CIO-SP contracts
Discount Rate	6 % real	OMB Circular A-94 midpoint (4–7 %)
Baseline ("As-Is")	• 46 prod VMs (8 vCPU / 32 GB) • 20 staging VMs • 24 FTE sustainment (GS-13 equiv.)	Current CMS ESB sustainment PoP (Feb 2025)
Cloud-Native ("To-Be")	• 18 K8s worker nodes + 3 control-plane • 14 FTE SRE sustainment	Mirrors 2024 HHS pilot
IaaS Unit Cost	$0.049 / vCPU-hr (AWS GovCloud IL4)	FY 25 GSA Cloud SIN
License Escalation	4 % CAGR proprietary vs. flat OSS	Gartner "Federal Software Price Index 2024"
Labor Rate	$164 k loaded / GS-13 FTE	FY 25 OPM GS + 37 % fringe
Automation Uptake	55 % Y1 → 85 % Y3	Based on HHS pilot DevSecOps metrics
One-time Compliance Cost	$300 k container STIG & SBOM buildout	DISA SRG baseline audits
Inflation / Escalation	2.2 % labor, 2 % cloud infra	OSD CAPE 2025–30 guidance
Exclusions (Neutral)	On-prem data-center depreciation, WAN backhaul	Same for both paths — cancels out
Risk-cost Reserve	$ 0.9 M (3 % PV)	Sum of mitigations R-1 … R-7

Category	Assumption	Rationale / Source
Schedule Reserve	5 calendar days	Trailing buffer for R-2 & R-4 activities

*Sensitivity test (± 15 % on labor rate, automation uptake, workload growth) keeps IRR between **22 % – 37 %**.*

A 3 % management reserve for risk mitigations and schedule buffer ($ 0.9 M, 5 days) is baked into the Cloud-Native column and reflected in the pessimistic scenario.

Appendix E – References

Executive Orders and Federal Mandates

1. **Executive Order 14028** – *Improving the Nation's Cybersecurity*
   White House, 2021
   https://www.whitehouse.gov/briefing-room
2. **Federal Zero Trust Strategy (OMB M-22-09)**
   Office of Management and Budget, 2022
   https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
3. **21st Century IDEA Act (P.L. 115-336)**
   U.S. Congress, 2018
   https://www.congress.gov

NIST Publications

4. **NIST SP 800-53 Rev. 5** – *Security and Privacy Controls for Information Systems and Organizations*
   https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
5. **NIST SP 800-37 Rev. 2** – *Risk Management Framework for Information Systems and Organizations*
   https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

6. **NIST SP 800-204** – *Security Strategies for Microservices-based Application Systems*
https://csrc.nist.gov/publications/detail/sp/800-204/final

7. **NIST SP 800-190** – *Application Container Security Guide*
https://csrc.nist.gov/publications/detail/sp/800-190/final

HHS and DoD/DHS Strategy Documents

8. **HHS IT Strategic Plan FY 2020–2025**
U.S. Department of Health and Human Services
https://www.hhs.gov/about/agencies/asa/ocio/strategic-plan/index.html

9. **DHS Cloud Strategy 2023**
Department of Homeland Security, Office of the CIO
https://www.dhs.gov

10. **DoD DevSecOps Reference Design**
DoD Enterprise DevSecOps Initiative, 2020
https://software.af.mil/dsop

11. **FedRAMP Program Management Office** – *Security Authorization and Guidance*
https://www.fedramp.gov

Commercial and Research White Papers

12. **Cloud Native Computing Foundation (CNCF)** – *State of Cloud Native Development Report*
CNCF, 2023
https://www.cncf.io/reports

13. **Red Hat** – *Modernizing Government IT with Containers and Kubernetes*
Red Hat Government Solutions, 2022
https://www.redhat.com

14. **IBM** – *Accelerating Federal DevSecOps Through Cloud Native Architectures*
IBM Center for the Business of Government, 2021
https://www.ibm.com/thought-leadership

15. **Gartner** – *Cloud-Native Platforms: Enabling Public Sector Agility*
Gartner Research, 2022
https://www.gartner.com