

Case Study | HealthTech and Agentic AI

Building a zero-trust mental health app with agentic AI in weeks, not months

How NeuroVitals used Atsign AI Architect to safely leverage AI agents, shipping a secure, identity-based healthcare application end-to-end in record time.



<100
Hours

of security debt engineering saved

~3
Hours

From concept → Operational MVP

EXECUTIVE SUMMARY

NeuroVitals is a mobile-first mental health and wellness platform that handles highly sensitive Protected Health Information (PHI), including lab results, clinical API data, mood tracking, and voice journals.

Faced with a strict timeline to launch a **100-user pilot**, NeuroVitals needed to build rapidly without compromising **HIPAA-level security** or **patient privacy**.

THE RESULT

By leveraging Atsign Platform and AI Architect, NeuroVitals safely utilized agentic AI to scaffold the application, accelerating their entire product launch roadmap from September to May. The partnership delivered an operational MVP in just three hours, saved over 100 infrastructure engineering hours, and established a decentralized architecture where encryption, identity management, and data security are built-in by default.

Healthcare innovation under pressure

AI is now the dominant investment theme in HealthTech, capturing 46% of all healthcare venture investment in 2025. But every CTO building agentic AI faces the same governance problem: agents processing PHI have no cryptographic identity, no defined authority scope, no auditable decision log, no custodial kill switch, and no defence against prompt injection. Every one of those gaps blocks a deal, fails a regulator, or worries an investor.

Compressed launch schedules

The company needed to compress a traditional multi-month enterprise development pipeline to achieve critical pilot deadlines while meeting industry compliance regulations.

Core product focus

The product team wanted to ensure that their valuable DevOps resources maximised their time spent on user-experience enhancing features, not security-debt.

Critical data sensitivity

Processing biometric data and qualitative mental health records meant a centralized data breach would be catastrophic, making cryptographic KYC identity & non-custodial encryption essential.

The AI security gap

AI Coding assistants accelerate build, but bolting on an agentic security stack (WAF, IdP, gateways, guardian agents) leaves data vulnerable increases time to launch & TCO

The healthcare innovation challenge

Stitching together WAF, IdP, secrets management, API gateways, reverse proxies, and guardian agents is a separate licence, integration and operational burden that unpredictably extends product launch time and costs.

Cryptographic KYC identity for every agent

To eliminate the risk of centralized data breaches, NeuroVitals abandoned the traditional cloud-database model. Instead, they built a cross-platform on Flutter mobile application powered by Atsign's identity-based architecture.

Every participant, including patients, practitioners, the application itself, and external clinical APIs, was assigned an Atsign. Data now moves directly between authenticated identities via end-to-end encrypted channels over a decentralized infrastructure. Because Atsign Platform is a zero-knowledge architecture, the routing servers cannot decrypt or view the traffic. As a result, there is no central honeypot of plaintext PHI for attackers to target.

The agentic workflow



Visual system mapping

NeuroVitals fed PRDs and workflow diagrams into an LLM to generate an architecture map. Imported into Atsign AI Architect, this created a complete, visually navigable layout of patients, practitioners, APIs, and data flows.



Agent-driven generation

The AI Architect output was passed to Claude Code, which autonomously scaffolded the application with Atsign's secure hooks natively wired in.



Instant secure activation

Once live Atsigns were provisioned, the AI swapped stubbed identities for live cryptographic keys. Fully encrypted PHI exchange worked on the first test.

"As the only engineer building it, could I have had the bandwidth, the time, or even the know-how to build all this stuff without Atsign there with me? The answer is straight up no."

— **Rick Deacon**
Head of Platform, NeuroVitals

Why HealthTech needs platform-layer security

For companies building workflows around vulnerable patient populations, privacy isn't just a compliance checklist; **it's a fundamental duty of care**. In the era of agentic AI, Atsign Platform abstracts the highest-risk engineering tasks away from the LLM. By moving cryptographic key management, secure transport, and identity authentication to the platform layer, AI agents can focus purely on business logic.

"With Atsign, you don't have to worry about the vast majority of that plumbing. It allows, especially in the age of agent coding, for you to not have to worry so much about things like encryption, data-layer security, and communication security."

— Rick Deacon,
18-Year Cybersecurity Professional and Head of Platform

Technical performance metrics	
	Time to market The platform accelerated the commercial product launch by four full months, pulling the timeline forward from September to May.
	Time to MVP The engineer completed the functioning application within approximately three hours of AI-assisted build time, delivering the initial project two days ahead of executive deadlines.
	Engineering economics Automating AI coding of Atsign's secure-by-design architecture saved >100 DevOps hours bolting-on bypassable WAF, IdP, API gateway, proxies & guardian agents security defenses.
	Team leverage A single engineer with an AI coding assistant achieved, in hours, achieved the total functional output of a multidisciplinary team spanning DevOps, SecOps, and backend engineering.
	Security posture Shifting to Atsign's decentralized peer-to-peer data exchange eliminated vulnerable centralized data silos and made healthcare regulatory compliance an architectural property.
	Stakeholder alignment The visual interface of AI Architect provided a shared language for clinical partners, executives, and engineering to validate core workflows instantly.

The takeaway for healthcare innovators

The NeuroVitals deployment demonstrates a significant shift in how we build complex business logic applications. By putting powerful development tools directly into the hands of subject matter experts, organizations can translate deep workflow nuances into production-ready software faster than ever.

For platforms handling PHI, clinical data, or financial integrations, Atsign Platform turns production-grade zero-trust security from a massive, multi-quarter engineering burden into a default property your application inherits on day one.

Layered-on agentic security stack	Structural agentic security stack
WAF Service Cloudflare, Nginx Edge traffic inspection IDP Service Okta, Entra ID Who gets in Secrets manager service HashiCorp Vault, CyberArk Credential vaulting API Gateway services Kong, Apigee Rate & Access control Guardian agents Services CrowdStrike, HiddenLayer Agents watching agents	Atsign Service Cryptographic KYC identity & Private Keys Who is acting and under what authority Authority-gated private encrypted messaging what they may do with who Every Runtime Action Verifiably Logged proof of what they did
Assumes trust by default and is by passable	No trust by default, no exposed endpoints to bypass
6+ services, 6+ contracts, 6+ failure modes, annual recurring runtime TCO	1 architecture, AI coder automatically integrated, no operations costs

3
Hours

Time to working MVP

4
Months

Launch pulled forward

0

Central PHI Honeypots

E2EE

Encryption always on by design