SECURING HEALTHCARE IOT ENVIRONMENTS WITH SOFTWARE SECURED

LOCATION

New york

INDUSTRY

Healthcare

EMPLOYEES

50-100

Alara is a fast-growing healthcare technology company that delivers secure edge orchestration software. We help hospitals and digital health platforms process PHI at the edge while supporting strict compliance needs across SOC 2, HIPAA, and HITRUST r2.

Navigating PHI Risk and Compliance Deadlines

Since their customers are health systems and digital health platforms, Alara requires uncompromising protection. Weaknesses in the gateway, control plane, or edge-deployed software could expose PHI, so validating their architecture and application was imperative.

When Software Secured was first introduced, Alara was preparing for a production-ready release that would significantly expand IoT capabilities. Meanwhile, they were also experiencing pressure to meet compliance requirements. They were navigating a demanding compliance roadmap spanning SOC 2, HIPAA, and HITRUST.

Past penetration tests had not delivered the depth Alara needed. As a startup, Alara didn't have the bandwidth to manage complex testing logistics. They needed a partner who could eliminate ambiguity and help them prioritize remediation without slowing product releases. The core ask was clear:

Expose risks early. Focus on healthcare IoT. Strengthen internet-facing components. Deliver clarity for compliance and audits. Stay within startup budget constraints.

Healthcare-Focused Test Plan

Alara selected Software Secured for its deep manual penetration testing and healthcare-focused pentest plan. They liked that the team received direct access to testers through a dedicated Slack channel. Testers validated assumptions early and helped Alara structure a clean test environment despite limited internal bandwidth.

SECURING HEALTHCARE IOT ENVIRONMENTS WITH SOFTWARE SECURED

Software Secured's unique light threat modeling, combined with the healthcare-specific pentest plan, shaped a custom attack plan tailored to Alara's UI, data flows, and healthcare context. This included business logic testing for unusual surfaces specific to healthcare data exchange protocols and the edge deployment lifecycle.
The team also calibrated severity scoring to the CVSS and DREAD standards,

providing developers with a rational framework for prioritizing work. Reports were actionable. Remediation guidance was specific and technically sound. Three rounds of retesting enabled Alara to sustainably fix issues. Integration with their compliance automation platform provided seamless SOC 2 evidence collection. A dedicated kickoff call, a detailed report readout, and continuous communication kept the process smooth.

A Scalable Security Foundation for Future IoT Growth

VSoftware Secured enabled the team at Alara to gain a complete, defensible understanding of their attack surface across IoT, the gateway application, and internet-facing components. The testers identified issues early, helping Alara avoid delays during client onboarding. Alara also received a public-facing penetration testing certificate, which reassured customers and aligned perfectly with SOC 2 and HIPAA expectations.

The high-touch process removed previous pain points. Communication was responsive. The Portal was easy to use. Technical explanations reduced internal friction and made remediation straightforward. By shifting towards a healthcare-aware test, Alara now operates with greater confidence in its security maturity.

Proven Protection for PHI Workloads

The engagement strengthened Alara's security posture across its IoT ecosystem and accelerated its compliance readiness for SOC 2, HIPAA, and HITRUST r2. By finding vulnerabilities early and validating fixes quickly, Alara avoided delays in product releases and confidently onboarded new customers.
Alara now manages risk for critical, internet-facing components with confidence. Their security program is stronger. Their attack surface is clearer. Their compliance pathway is smoother. Alara now proactively demonstrates maturity before clients request proof.

Software Secured continues to partner with Alara as they move into deeper authenticated application testing, supporting the security program as it grows.
All internet-facing components were validated as hardened before production release, giving Alara a confident and defensible security posture.