02 / 05 CYBERSECURITY & APPSEC HEALTHCARE TECHNOLOGY

Cybersecurity Remediation for a Digital Health Platform

A Boston-based digital health startup processing sensitive patient data discovered critical vulnerabilities in their web application ahead of a HIPAA compliance review. With patient data at risk and a compliance deadline 8 weeks out, Algebrix delivered a full application security assessment and remediation programme.

CLIENT PROFILE	ENGAGEMENT VALUE	DURATION	DECISION MAKER
Health Tech · 90 employees · Boston	**USD $29,500**	**8 weeks**	**CTO & Head of IT**

THE PROBLEM

The company's patient portal — used by 40,000 active users — was built rapidly during a funding push and had never undergone a formal security review. A third-party penetration test commissioned ahead of a HIPAA audit flagged 14 vulnerabilities including two critical-severity issues: an authentication bypass flaw allowing unauthenticated access to patient records, and an insecure direct object reference (IDOR) vulnerability exposing PHI across accounts. The company had 8 weeks to remediate before the compliance review. Their internal team had no application security expertise and the original dev agency was no longer available.

OUR APPROACH

1 **Triage & emergency patching**
In the first week, Algebrix triaged all 14 vulnerabilities, confirmed exploitability of the two critical issues, and deployed interim controls to block exploitation while permanent fixes were developed. No data breach occurred during the remediation window.

2 **Code-level remediation**
Fixed all 14 vulnerabilities at the source code level — not with perimeter controls — including a full re-architecture of the authentication flow, IDOR remediation with proper object-level authorisation, input validation hardening, and secure session management implementation.

3 **HIPAA security controls alignment**
Mapped all remediations to HIPAA Security Rule technical safeguard requirements (§164.312). Implemented audit logging for all PHI access, encryption at rest and in transit verification, and automatic session timeout controls.

4 **Security testing & validation**
Conducted post-remediation security testing to verify all fixes, producing a remediation evidence report suitable for the HIPAA compliance reviewer and establishing a secure development checklist for the internal team going forward.

OUTCOMES

14 / 14
Vulnerabilities fully remediated before the compliance deadline

0
Data breach incidents — critical issues contained within 5 days

HIPAA
Compliance review passed — platform cleared to scale to hospital clients

TECHNOLOGIES USED

OWASP Top 10 · Burp Suite · Node.js / React · JWT Authentication · AWS WAF · TLS 1.3 · HIPAA §164.312 · AES-256 Encryption

> *"We were in a serious situation — critical vulnerabilities in a platform holding patient data, eight weeks until our compliance review. Algebrix moved fast, communicated clearly at every step, and fixed everything properly at the code level rather than patching around it. They saved us from what could have been a catastrophic incident."*

— CTO, Digital Health Platform · Boston, USA (Illustrative)

READY TO WORK WITH ALGEBRIX?

Let's solve your next technology challenge.

Whether you're facing a compliance deadline, a legacy system holding you back, a security gap, or a product you need to build — we'd like to hear about it. Every engagement starts with a 30-minute discovery call, no obligation.

WEBSITE
www.algebrix.co

EMAIL
contact@algebrix.co

LINKEDIN
linkedin.com/company/algebrix

BOOK A DISCOVERY CALL →

Algebrix · Jahangir Danish LLC · Incorporated in Wyoming, USA · www.algebrix.co

All case studies above are illustrative engagement examples. Client names and identifying details are not disclosed.