ENCRYPTION CONSULTING

CASE STUDY

COMPLIANCE SERVICES

A clear path to FIPS 140-2 for a healthcare giant

A top US healthcare provider with more than 20,000 employees and a global client database set out to achieve FIPS 140-2 compliance. Our assessment examined its cryptography end to end and mapped every gap, with a structured path to certification.

SECTOR	SIZE	ENGAGEMENT
Healthcare (US)	20,000+ employees	FIPS 140-2 assessment

FIPS 140-2
Certification achieved

AES-256
RSA-2048 adopted

MFA
On key systems

A healthcare giant, 20,000 strong

We worked with one of the top healthcare providers in the USA, offering a wide portfolio of health insurance and services to people nationally and internationally. It manages a global database of thousands of clients and their confidential information.

With multiple locations, more than 20,000 employees, and continuous communication channels across hospitals and clinics, the organization set out to achieve FIPS 140-2 compliance. It needed a thorough assessment across its wide infrastructure to guide every step toward meeting the standard.

In healthcare, protecting PII and PHI isn't optional. FIPS 140-2 is how this organization set out to prove its cryptography could be trusted.

Cryptographic gaps, against the standard

A FIPS 140-2 gap assessment of the cryptographic environment surfaced exposed data, shared keys, and weak controls.

1

Unencrypted databases

Several Oracle and SQL Server databases stored sensitive data with no encryption applied, leaving PII and PHI exposed.

2

A single shared key

One encryption key protected many applications, services, and backups, so breaching one system could compromise them all.

3

No role-based access

Without RBAC or IAM, access was over-provisioned, making it far easier than it should be to reach sensitive keys and data.

4

Misaligned crypto policies

Policies didn't align with FIPS 140-2, with outdated algorithms, weak cipher suites, and key sizes too small to resist modern attacks.

5

Poor key management

Weak access controls, a single key reused across services, and no monitoring of key usage all raised the risk of keys being exposed through sharing, misconfiguration, or simple oversight.

> The organization's cryptographic environment had grown without a compliance-focused strategy. The assessment provided the clarity needed to identify every gap and build a structured path to FIPS 140-2 certification.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · COMPLIANCE SERVICES

A structured path to FIPS 140-2

Our gap analysis mapped each application's data flows and showed exactly where the organization stood against FIPS 140-2, then turned every finding into a concrete recommendation.

Data-flow gap analysis

We mapped each application's data flow from ingress to egress, at rest and in transit, to pinpoint every gap against FIPS 140-2.

FIPS-aligned policies

We updated cryptographic policies and module specifications to align with FIPS 140-2, so current and future applications follow the standard.

Modern encryption everywhere

AES-256 and RSA-2048 protect data at rest and TLS 1.2 or higher protects data in transit, securing information at every touchpoint.

Unique keys per app

Each application gets its own encryption key, isolating systems so a single breach can't cascade across the environment.

RBAC, IAM, and MFA

Least-privilege access through RBAC and IAM across on-prem and cloud, plus MFA on cryptographic systems and key management interfaces.

Secure key lifecycle in HSMs

A full key lifecycle, generation, rotation, and revocation, with keys stored in HSMs and key vaults and usage monitored throughout.

Certified, secure, and ready to grow

The assessment and remediation plan took the organization to FIPS 140-2 compliance, strengthening its security posture and protecting patient data more effectively.

0

Unencrypted databases remaining

BEFORE — no encryption

AFTER — AES-256

FIPS 140-2 certified

Standardized encryption and controls earned the organization FIPS certification, cutting the risk of costly breaches and fines.

PHI better protected

Sensitive patient information is now protected at every touchpoint with FIPS-compliant encryption and stronger access controls.

New partnership doors

FIPS compliance opened opportunities for strategic partnerships with technology suppliers and other healthcare providers.

Compliance, sustained

Security best practices are now embedded in daily operations, reducing the risk of future non-compliance.

IN SUMMARY

A compliant base, built for better care

For a healthcare provider trusted with PII and PHI, FIPS 140-2 is proof that cryptography can be relied on. Our assessment mapped the organization's data flows, ran a detailed gap analysis, and turned every finding into a concrete plan. By updating policies to the standard, enabling AES-256 and RSA-2048 with TLS 1.2 and above, isolating applications with unique keys, tightening access through RBAC, IAM, and MFA, and securing the full key lifecycle in HSMs, the organization achieved FIPS 140-2 compliance. It now protects patient data more effectively, has opened doors to new partnerships, and has security best practices embedded for years to come.

GET STARTED

Get ready for FIPS 140-2.

Talk to our compliance team →