ENCRYPTION CONSULTING

CASE STUDY

CODE SIGNING SECURITY

Securing every release in a healthcare pipeline with CodeSign Secure

A respected US healthcare institution was shipping software with no code signing, no build verification, and no vulnerability scanning. We integrated CodeSign Secure into their Jenkins pipeline to make every release trusted and compliant.

SECTOR	ENVIRONMENT	SOLUTION
Healthcare (US)	Jenkins CI/CD	CodeSign Secure

HIPAA
Compliance met

10%
Vulnerability upload gate

FIPS Level 3
HSM-backed key storage

A healthcare leader, built on patient trust

Our client is a well-respected healthcare institution running a comprehensive system of hospitals, clinics, and research facilities. Every day it handles sensitive patient information and critical procedures, and it is known for its commitment to patient-friendly technology.

As an organization the healthcare sector relies on, it has to uphold strict monitoring, data protection, and operational standards. But one major gap remained in its security posture: it had no code signing, leaving room for tampered or malicious code to slip in through a software update or application.

In healthcare, unverified software isn't just a bug risk. It's a direct threat to patient data and the systems that care for people.

Unverified software, in a high-stakes industry

The healthcare firm had real gaps in how its software was signed, built, and checked, with patient data on the line.

1

No code signing

They couldn't integrate code signing into their existing Jenkins pipeline, relying on manual verification and leaving their CI/CD process exposed.

2

Reproducible builds

They needed every build to produce identical artifacts regardless of environment, since minor inconsistencies invite debugging pain, tampering, and compliance gaps.

3

CI/CD bottlenecks

Code vulnerabilities and a web of internal and external dependencies dragged on performance and reliability, making SBOM-based scanning essential.

4

Unverified, non-compliant code

Without signing and verification, altered or unauthenticated code could ship, risking HIPAA and GDPR compliance and exposing patient data.

5

Secure keys and HIPAA from day one

Any solution had to store private keys securely, slot into Jenkins build triggers without retraining, and meet healthcare standards like HIPAA from the start.

> The organization had no code signing, no build verification, and no vulnerability scanning; every piece of software leaving the pipeline was an unverified trust assumption in an industry where patient data is at stake.

ENGAGEMENT SUMMARY: ENCRYPTION CONSULTING · CODESIGN SECURE

From unsigned builds to verified releases

We deployed CodeSign Secure directly into their Jenkins pipeline, adding signing, build verification, and vulnerability scanning without disrupting how the team already worked.

Works with existing Jenkins

CodeSign Secure slotted into their current Jenkins pipeline, so the team kept its setup and skipped heavy retraining on new tools.

Reproducible builds

We configured reproducible builds so every compile produces identical artifacts, a matching hash, no matter the environment.

Pre-sign hash validation

The pipeline validates the code's hash before signing, confirming its integrity is intact at the exact moment of signing.

SBOM vulnerability scanning

SBOM-based scanning checks code for vulnerabilities before it ever reaches GitHub, catching issues at the earliest stage.

A 10% vulnerability gate

If code exceeds a 10% vulnerability threshold, the upload is blocked, stopping unsafe code before it can move down the pipeline.

HSM key protection

Signing keys live in tamper-resistant HSMs from vendors like Thales, Utimaco, and nCipher, safe from corruption, theft, or misuse.

Every release, signed and verified

With CodeSign Secure in place, the firm could prove the integrity of every build and ship software the healthcare sector can trust.

0

Unverified code reaching production

BEFORE — manual checks

AFTER — automated signing

Signed audit trails

Comprehensive, signed audit logs bring transparency and accountability to every signing event, ready for compliance reporting.

Trusted timestamps

RFC 3161 and Authenticode timestamps secure every signature, keeping software integrity verifiable for the long term.

HIPAA and CA/B Forum

FIPS 140-2 Level 3 HSMs and automated controls let the firm meet HIPAA and the CA/Browser Forum's June 2023 requirement.

Less risk, fewer errors

Automated vulnerability detection minimized human error, making sure unsafe code never reaches end users.

IN SUMMARY

Trusted software, built for healthcare

For a healthcare organization, protecting patient data and software integrity is everything. CodeSign Secure resolved the firm's biggest gaps, integrating signing, reproducible builds, pre-sign hash validation, and SBOM scanning directly into their Jenkins pipeline, with a 10% vulnerability gate and FIPS 140-2 Level 3 HSMs protecting their keys. Signed audit trails and trusted timestamps keep every signature verifiable, and the firm now meets HIPAA and CA/Browser Forum requirements with confidence. Only unaltered, secure software reaches end users, and trust in the supply chain stays intact.

SEE IT IN ACTION

Sign every build with confidence.

Book a Codesign Secure Demo →