



Pharmaceutical Research Cloud Migration

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1

HIPAA-Compliant Hybrid Cloud for Clinical Data: Zero-Data-Loss Migration and 40% Storage Savings

1

1.1

Executive Summary

1

1.2

The Challenge

1

1.3

Our Approach

2

1.4

Implementation

3

1.5

Results & Impact

4

1.6

Technologies & Services Used

4

1.7

Conclusion

5

About The Origami Corporation

1

HIPAA-Compliant Hybrid Cloud for Clinical Data: Zero-Data-Loss Migration and 40% Storage Savings

1.1

Executive Summary

A fast-growing biotech research company needed to modernize how it stores and accesses clinical datasets containing protected health information (PHI). Their on-premise environment was costly, difficult to scale, and inconvenient for researchers collaborating across multiple sites. The mandate: migrate to the cloud without compromising HIPAA compliance, data integrity, or performance.

We delivered a hybrid architecture that places PHI on dedicated, compliant servers while shifting archival and research-optimized datasets to encrypted cloud storage. Through a staged cloud-migration program coupled with a HIPAA compliance audit, disaster recovery design, and ongoing managed services, the client achieved a seamless transition with zero data loss, reduced storage costs by 40%, and significantly faster data access from multiple locations—all while strengthening audit readiness and operational resilience.

1.2

The Challenge

The client’s on-premise infrastructure was reaching its limits:

- Sensitive clinical datasets (PHI) were growing rapidly, saturating local storage arrays and backup windows.
- Researchers across three sites needed low-latency, secure access to large datasets for analysis and collaboration.
- Existing controls were not fully aligned with HIPAA Security Rule expectations for audit controls, transmission security, and integrity.

- The organization lacked a tested disaster recovery posture and struggled with lengthy restore times.
- Any migration risked downtime and data loss—both unacceptable for active clinical research timelines.

The client required a HIPAA-compliant solution that could:

- Segregate PHI from de-identified and archival data.
- Provide secure, performant access for multi-site research teams.
- Reduce storage and operations costs.
- Improve auditability, governance, and resilience.
- Transition with zero data loss and minimal disruption.

1.3 Our Approach

We implemented a phased program blending cloud-migration, compliance, and operational transformation:

1. HIPAA Compliance Audit and Readiness

- Conducted a HIPAA security risk assessment and gap analysis covering administrative, physical, and technical safeguards.
- Validated Business Associate Agreement coverage and updated policies for access control, breach notification, data retention, and minimum necessary use.
- Designed evidence collection and audit trails to meet HIPAA audit requirements.

2. Data Classification and Architecture Blueprint

- Classified datasets into PHI, de-identified working sets, and long-term archives.
- Proposed a hybrid model: dedicated servers for PHI, cloud object storage for archives, and cloud block/file storage for de-identified datasets and research workloads.
- Defined security controls: encryption (in transit and at rest), network segmentation, identity and access management (IAM), logging, and DLP.

3. Migration and Cutover Strategy

- Employed a staged migration with pre-migration synchronization, validation, and a controlled final cutover.
- Implemented integrity checks (checksums and hash validations) to guarantee zero data loss.
- Coordinated change windows with research schedules to avoid disruption.

4. Resilience and Managed Services

- Architected disaster recovery with cross-region replication for critical datasets and runbook-driven failover.
- Transitioned ongoing operations to managed services: 24x7 monitoring, patching, backups, cost optimization, and quarterly HIPAA control reviews.

1.4 Implementation

Architecture and Security Controls - Dedicated PHI Enclave: Deployed dedicated bare-metal servers in a HIPAA-ready, SOC 2 Type II compliant data center. The enclave used self-encrypting drives, FIPS 140-2 validated encryption modules, and a private network segment with strict firewall rules and microsegmentation to limit lateral movement. - Cloud Storage for Archives and Non-PHI: Provisioned cloud object storage for long-term archives with server-side encryption (AES-256), customer-managed keys in a hardened key management service (KMS/HSM), and lifecycle policies that tier older data to colder, cost-optimized storage. WORM/immutable object lock and MFA delete were enabled for legal hold and ransomware resistance. - Research Data Tier: Hosted de-identified datasets in cloud block/file storage for analytics workloads. Implemented read-optimized storage options and regional replication to reduce access latency for multi-site teams. - Secure Connectivity: Established redundant site-to-cloud connectivity via IPsec VPN with failover, complemented by private connectivity for sensitive synchronization. Network ACLs and security groups enforced least privilege at every layer. - IAM and SSO: Integrated SAML 2.0 SSO for researchers and administrators, with role-based access control, just-in-time provisioning, and MFA enforcement. Administrative actions required privileged access workflows and session recording. - Logging and Monitoring: Centralized logs (system, access, network, and application) into a SIEM for real-time alerting, correlation, and audit reporting. Retention policies supported HIPAA recordkeeping requirements.

HIPAA Compliance and Governance Enhancements - Access Controls: Implemented least-privilege IAM roles, break-glass procedures, and just-in-time elevation for administrative tasks. - Audit Controls: Enabled immutable audit logs, comprehensive API activity tracking, and regular review procedures. Dashboards automated evidence pack creation for auditors. - Integrity and Transmission Security: Enforced TLS 1.2+ for all transfers; integrity checks with SHA-256 hashes verified at each migration stage. File-level integrity monitoring highlighted unauthorized changes. - Data Loss Prevention: Applied content-aware scanning for PHI on egress channels and storage buckets, with automated quarantine and alerting.

Migration Execution - Pilot and Validation: Migrated a representative dataset to validate performance, access controls, and tooling. Addressed edge cases (file path normalization, metadata preservation, and research pipeline compatibility). - Synchronization and Cutover: Used a combination of parallel rsync, database replication/CDC where applicable, and snapshot-based transfers. Conducted iterative

syncs to minimize cutover deltas. Final cutover executed during a planned window with rollback checkpoints defined. - Verification: Post-migration, we ran dataset-wide checksum comparisons, sample reads, and application-level validations. Researchers verified workflow continuity before decommissioning legacy storage.

Disaster Recovery and Business Continuity - Strategy: Implemented cross-region replication for critical datasets, immutable backups adhering to the 3-2-1 rule, and automated infrastructure-as-code (IaC) templates for rapid environment rebuilds. - Testing: Conducted tabletop exercises and a controlled failover test with documented RTO/RPO expectations and runbook refinements. - Recovery Posture: Established regular backup verification, quarterly DR drills, and air-gapped backup copies to mitigate ransomware risks.

Operationalization via Managed Services - 24x7 Monitoring and Incident Response: Proactive alerting on performance, security events, and cost anomalies with defined incident SLAs. - Patch and Configuration Management: Baseline hardening, CIS-aligned configurations, and automated patching windows coordinated with research timelines. - Cost Optimization: Storage tiering, rightsizing, and lifecycle updates continuously tuned to maintain savings without compromising performance.

1.5 Results & Impact

- Zero Data Loss: The migration achieved complete data integrity, confirmed through checksum validation and application-level testing.
- 40% Storage Cost Reduction: Lifecycle policies, object storage utilization, and archival tiering reduced storage spend by 40% compared to the prior on-premise footprint.
- Faster Multi-Site Access: Researchers experienced significantly faster data access from multiple locations due to regional replication, optimized storage tiers, and secure low-latency connectivity.
- Strengthened HIPAA Posture: Access controls, immutable audit trails, encryption, and formalized policies improved audit readiness and reduced compliance risk.
- Resilient Operations: With disaster recovery, immutable backups, and managed services, the client gained a robust continuity posture and predictable operational support.
- Research Agility: The hybrid model enables rapid onboarding of new studies, scalable storage for growing datasets, and secure collaboration without infrastructure bottlenecks.

1.6 Technologies & Services Used

- Cloud-Migration

- Staged synchronization (rsync, snapshot transfer, CDC), checksum validation, pilot cutovers, and rollback planning
- Infrastructure-as-code for repeatable environments
- Compliance-Audit-HIPAA
 - HIPAA risk assessment, policy updates, BAA review, audit evidence automation, DLP controls
 - Centralized logging, immutable audit trails, and access review workflows
- Dedicated-Servers
 - HIPAA-ready data center, bare-metal with self-encrypting drives, FIPS-validated crypto, microsegmentation, private networking
- Disaster-Recovery-Services
 - Cross-region replication, immutable backups (WORM/MFA delete), DR run-books, failover testing, 3-2-1 strategy
- Managed-Services
 - 24x7 monitoring and incident response, patch/configuration management, cost optimization, quarterly compliance reviews
- Supporting Capabilities
 - KMS/HSM for key management, TLS 1.2+ encryption, SAML SSO with MFA, SIEM integration, network firewalls and IDS/IPS, lifecycle policies for tiered storage

1.7 Conclusion

By combining a HIPAA-aligned compliance program with a pragmatic hybrid architecture, we enabled the biotech client to move sensitive clinical data to a modern, secure platform without sacrificing integrity or performance. The result: a zero-data-loss migration, 40% lower storage costs, faster access for distributed research teams, and a sustainable operational model backed by disaster recovery and managed services. This foundation positions the organization to scale confidently, accelerate discovery, and meet regulatory obligations as their research portfolio grows.

About The Origami Corporation

The Origami Corporation is a leading technology consulting firm specializing in cloud migration, DevSecOps, cybersecurity, and digital transformation. We help organizations navigate complex technological challenges and achieve their business objectives through innovative, secure, and scalable solutions.

Connect With Us

Follow Us Online

LinkedIn: [The Origami Corporation](#)

Facebook: [@theorigamicorporation](#)

X (Twitter): [@OrigamiGlobal](#)

Telegram: [@theorigamicorporation](#)

Contact Information

Europe & Americas

- **Email:** office@theorigamicorporation.com
- **Phone:** +359 878 686 627

Asia-Pacific, Middle East & Africa (APMEA)

- **Email:** office.apmea@theorigamicorporation.com
- **Phone:** +41 77 924 2245

Ready to Get Started?

SCHEDULE A MEETING

Ready to transform your technology infrastructure? Contact us today to discuss how we can help your organization achieve similar results.