

CUSTOMER SUCCESS STORY

Private AI on patient data, inside the boundary.

A health system wanted clinical AI — summarisation, retrieval over the record, imaging support — without patient data reaching an external model service. **UPC Sovereign** supplied dedicated GPUs inside the same perimeter as the data.

PHI in-boundary

AI changed the sovereignty question. It was no longer only where records are stored, but where prompts, embeddings, model weights, and inference execution live — and whether an AI agent's access can be constrained as tightly as a clinician's.

THE SITUATION

Clinical AI kept failing the same review

Each proposed AI workload cleared its clinical evaluation and then stalled at information governance for the same reasons:

- **Inference meant export.** Using external model services would move PHI outside the boundary, prompts and embeddings included.
- **Derived data was unaddressed.** Fine-tuned weights derived from patient records carried the same obligations as the records.
- **Agent access was unbounded.** Retrieval pipelines and agents could reach systems with no enforceable identity or execution limit.
- **Lineage could not be shown.** The system could not evidence which data trained which model, or who approved it.

THE DECISION

Bring the GPUs inside the perimeter

The health system deployed dedicated GPU clusters within its sovereign boundary, so training and inference execute where the data already sits, under the same access and audit regime.

“We were never going to win approval to send patient records to an external model. The only path was to run the model where the records already live.”

— CHIEF INFORMATION & DIGITAL OFFICER

DEPLOYMENT SNAPSHOT

SECTOR

Integrated health system with research arm

WORKLOADS

Clinical summarisation · Record RAG · Imaging support

EDITION

UPC AI-Optimized Sovereign Cloud

COMPUTE

Dedicated GPU clusters inside the perimeter

ENCRYPTION

In transit and during model training

GOVERNANCE

Data lineage documentation, EU AI Act mapping

ACCESS

Enforceable identity and execution boundaries

RESILIENCE

In-boundary backup and DRaaS

WHAT SITS INSIDE THE BOUNDARY

Data

Patient records, imaging archives, and the **prompts, embeddings, and derived weights** generated from them — all held to one residency rule.

Compute

Dedicated GPU clusters within the sovereign perimeter, with processing pipelines for model training and inference.

Encryption

End-to-end encryption **in transit and during model training**, with customer-controlled keys.

Governance

Data lineage documentation and EU AI Act compliance mapping, plus enforceable identity, network, and execution boundaries for agents.

WHAT CHANGED

BEFORE UPC SOVEREIGN

- Inference would **export PHI** to external services
- Derived weights and embeddings ungoverned
- Agent and retrieval access effectively unbounded
- No documented lineage from data to model
- Each AI proposal re-litigated at governance

WITH UPC SOVEREIGN

- Training and inference run **inside the boundary**
- Derived artefacts carry the same residency rule
- Agents operate within **enforceable** execution limits
- Data lineage documented and inspectable
- A reusable governance pattern for new workloads

WHERE THE ASSURANCE CAME FROM

Compute moved to the data

Dedicated GPUs inside the perimeter removed the export requirement entirely, which is what converted a blocked programme into an approvable one.

Derived data treated as regulated

Extending residency to prompts, embeddings, and fine-tuned weights closed the gap most AI programmes leave open.

Bounded agents

Enforceable identity, network, and execution boundaries let autonomous components operate without inheriting unlimited reach.

WHY THIS MATTERS IN HEALTHCARE

Controls and frameworks doing the work in this deployment:

PHI in-boundary

HIPAA alignment

Encryption during training

Data lineage

EU AI Act mapping

Bounded AI agents

Customer-owned keys

In-boundary DR

BOTTOM LINE

UPC Sovereign let a health system run clinical AI on patient data without that data, or anything derived from it, leaving the boundary.

Build your sovereign cloud strategy with UPC.

Speak with a specialist, or ask us to map your residency and jurisdictional requirements.

UPC SOVEREIGN™

UNITEDLAYER.COM



EMAIL

contact@unitedlayer.com



PHONE

[+1-888-853-7733](tel:+1-888-853-7733)



X

x.com/unitedlayer



LINKEDIN

linkedin.com/company/unitedlayer