COMPEX / SECTOR EVIDENCE SUMMARY

# Healthcare & Hospitals

A synthetic demonstration bundle showing the exact evidence shape a production Compex run exports: signed contract, hardware attestation and an ordered hash chain of every allowed and blocked operation.

| BUNDLE | CONTRACT | ATTESTATION |
|---|---|---|
| EV-HLT-2026-11-001 | PC-HLT-2026-11 | NVIDIA H100 Confidential Computing |

## Pipeline Contract

| | |
|---|---|
| **Purpose** | Clinical diagnostic support + cohort matching |
| **Data owner** | Hospital Data Owner |
| **Reviewer** | DPO / Clinical Governance |
| **Allowed columns** | deidentified_lab_values, imaging_embeddings, cohort_id, encounter_type, age_band |
| **Blocked columns** | patient_mrn, patient_name, raw_clinical_notes |
| **Command allow-list** | read_deidentified_columns, run_diagnostic_model, match_cohort |
| **Output limit** | diagnosis_probability + cohort_count; no PHI |
| **Retention** | 0 days in enclave; bundle retained 10 years |

**contract_hash**

```
49d709b8d02fd899600ba8db35604ed07a6dc055f160e186d7069caf16350ffc
```

## Hardware attestation

| | |
|---|---|
| **TEE type** | NVIDIA H100 Confidential Computing |
| **Verification** | GPU attestation report verified \| report_data binds the contract hash and the diagnostic model digest |

**tee_attestation_quote**


```
V/0QpUCTK/spbTYMvz6eomddRMCgrY48RCKeFiFbNyZX/RClQJMr+yltNgy/Pp6iZ11EwKCtjjxEIp4WIVs3Jg==
```


## Deployment profiles

| LAYER | CLOUD CONFIDENTIAL VPC | ON-PREMISE / AIR-GAPPED |
|---|---|---|
| Data lives in | A sovereign cloud enclave inside the hospital's VPC, next to the EHR. | Hospital-owned GPU servers behind the clinical firewall, including air-gapped research wings. |
| TEE hardware | AWS Nitro Enclaves; Azure/GCP Confidential VMs on AMD SEV-SNP or Intel TDX; NVIDIA H100 confidential GPUs for imaging. | Bare-metal AMD EPYC (SEV-SNP), Intel Xeon (TDX) and NVIDIA H100/Blackwell GPU TEEs over encrypted PCIe. |
| Locked out | Cloud provider admins, the host OS/hypervisor and the external AI vendor. | Internal root sysadmins, hypervisor operators and third-party model/agent developers. |
| Egress | VPC-peered zero-egress subnet; keys are released only after the attestation quote matches the contract. | Strictly air-gapped: 0.0.0.0 outbound blocked. The local verifier checks the silicon signature offline. |

Evidence bundle

# Execution hash chain

Every permitted read and every refused operation is written in order. The chain head is signed by the TEE.

| SEQ | TYPE | EVENT | SHA-256 |
|---|---|---|---|
| 001 | CONTRACT | Pipeline Contract PC-HLT-2026-11 verified against the DPO/clinical governance signature. | ed2f8459e490cca1a900... |
| 002 | ATTEST | NVIDIA H100 confidential-computing report verified; report_data binds the contract hash. | ba51b2ff3ecc65939ba7... |
| 003 | READ | Allow-listed read: deidentified_lab_values, imaging_embeddings, cohort_id, encounter_type, age_band. | 77b4ef9eb4d408a83023... |
| 004 | OUTPUT | Signed output released: diagnosis_probability and cohort_count only. | 7ebf7eb966f8c65d4bfc... |
| 005 | BLOCKED | Out-of-scope write refused: patient_mrn in intermediate weights. | 4824bf5741ab33c15af4... |
| 006 | BLOCKED | Egress blocked: pip install https://external.example/cohort-tools. | 5f37157a4f4789ecb8d9... |
| 007 | SEALED | Evidence bundle sealed; hash chain head signed by the TEE. | 4c02f88fc29c10c3068a... |

## Files in this bundle

| FILE | SIZE | SHA-256 (synthetic) |
|---|---|---|
| evidence.json | 4 KB | f647c29d9c37ac6e774020fa1760ad3d7584... |
| summary.pdf | 7 KB | 5d2a3bc0f6a38ea077247ff785be58b83b5d... |
| audit.csv | 2 KB | f4ae2a3e9da9fe8078dce7ea318bdbae525c... |

Synthetic demonstration bundle. No customer data is included. Compex produces technical evidence of how a workload executed; legal conclusions are yours.