CONFIDENTIAL COMPUTING CONSORTIUM

USE CASE:
Healthcare & Precision Medicine

Executive Summary

Healthcare organizations increasingly need to collaborate across hospitals, research institutions, and pharmaceutical companies to train AI models on larger and more diverse patient populations. However, patient privacy regulations (HIPAA, GDPR, regional health-data laws) can make centralized data sharing difficult.

Confidential Computing was used at UPenn to enable collaborative AI development while protecting patient data during computation, creating an environment where sensitive healthcare information remains encrypted and inaccessible even to infrastructure operators.

Challenge

A consortium of healthcare researchers and institutions sought to develop predictive AI models for brain tumor disease detection and treatment optimization using geographically distributed patient datasets.

The University of Pennsylvania started with just a few hundred publicly available brain scans and needed a way to securely collaborate with dozens of research institutions. Traditional approaches created major obstacles: patient data could not be centrally pooled, researchers required access to insights without accessing raw patient records, existing encryption protected data at rest and in transit but not during computation, and participating institutions lacked sufficient trust to expose sensitive datasets to shared cloud environments.

How Confidential Computing Was Implemented

Federated Learning alone prevents raw data sharing, but model updates can still unintentionally leak information about patient records. UPenn and other teaching hospitals needed Confidential Computing to build Trusted Execution Environments (TEEs) to protect model aggregation, intermediate computations, and patient-derived model updates.

This protects data while in use, eliminating one of the largest remaining attack surfaces in collaborative healthcare AI. The research was validated using more than 3.7 million images from over 6,000 patients across 71 participating healthcare sites worldwide.

Organizations that previously could not share data due to compliance concerns were able to contribute to collaborative model development. Researchers gained access to more diverse patient populations without moving patient records.

Results & Key Takeaway

Confidential Computing transformed a privacy-constrained healthcare collaboration problem into a scalable research ecosystem by protecting patient data during active computation.

By using Confidential Computing, researchers were able to improve cancerous brain tumor detection by 33%.

Sources

1. Nature: Optimization of Cross-Institutional Medical Federated Learning - nature.com/articles/s41598-026-44843-4
2. UPenn Uses Confidential Computing to increase brain tumor detection
3. ScienceDirect
4. FeTS Initiative: Federated Tumor Segmentation open-source platform for collaborative AI on protected patient populations