CONFIDENTIAL COMPUTING CONSORTIUM

USE CASE:
Confidential AI for Pharmaceutical Research & Drug Discovery

Executive Summary

Drug discovery has become one of the world's most capital-intensive and high-risk industries, with individual drug development costs averaging billions of dollars. Research organizations face intense pressure to accelerate development timelines, lower clinical failure rates, and identify viable therapeutic candidates before investing heavily in physical laboratory trials.

AI-driven molecular analytics and large language models (LLMs) have emerged as a scalable alternative to traditional trial-and-error screening, enabling researchers to evaluate data effectiveness faster and at a lower cost. However, the effectiveness of these models depends heavily on access to massive, diverse datasets. In practice, many of the most valuable biomedical datasets remain inaccessible because of stringent global privacy regulations, intellectual property boundaries, and commercial concerns surrounding proprietary molecular formulas and research models.

Confidential Computing addresses this challenge by enabling organizations to collaborate on AI training and analytics while maintaining absolute control over sensitive data. By protecting data during active computation and providing verifiable assurances about how it is processed, Confidential Computing allows multi-party research initiatives to drive innovation without exposing underlying datasets.

Business Challenge

A specialized drug discovery organization collaborated with five leading pharmaceutical companies to leverage advanced AI and LLM workloads to accelerate therapeutic development. The initiative sought to pool disparate biomedical datasets and proprietary research models to improve the predictive accuracy of their algorithms.

While individual datasets provided limited scope, combining data from multiple stakeholders promised to unlock significant R&D breakthroughs. However, three critical constraints blocked standard data-centralization approaches:

Regulatory Compliance - The highly confidential and sensitive nature of genomic and clinical records meant strict compliance with global privacy regulations was mandatory.

Commercial Secrecy - Participating companies lacked technical guarantees that their highly proprietary datasets and discovery models would remain protected from competitors.

The Processing Gap - Traditional cloud security approaches safeguarded data at rest and in transit, but left sensitive information exposed in memory during active computation.

As a result, the structural realities of modern R&D, where costs average $1 billion to $2 billion per new drug, success rates hover below 1%, and development lead times stretch between 10 to 20 years, remained a binding constraint that data sharing could not safely solve.[1]

How Confidential Computing Addressed the Need

The solution was deployed on an advanced, confidential hardware infrastructure, creating hardware-protected Trusted Execution Environments (TEEs) for intensive AI training and analytics workloads.

Within these secure environments, data sharing, access control, and key management systems operated seamlessly to protect data throughout the entire processing lifecycle:

- Hardware-Based Attestation - Data owners could cryptographically verify the integrity of the execution environment and deployed AI models before authorizing access to their data.
- Zero-Trust Integrity - This verification ensured that only pre-approved code could process information, keeping raw records completely inaccessible to cloud providers, platform operators, or unauthorized insiders.
- Workflow Governance - Unified management workflows allowed participants to define, track, and enforce privacy and security guardrails interactively without revealing raw inputs to other participants.

By shifting trust from traditional contractual agreements to cryptographic verification, Confidential Computing fundamentally changed the multi-party collaboration model. Organizations that were previously unwilling to risk their intellectual property gained the technical assurances required to participate.

Results & Business Value

With Confidential Computing in place, the research consortium successfully bypassed traditional data silos to unlock immense operational and financial value:

- Model Accuracy Boost - By enabling secure data collaboration, the available training foundation expanded significantly, improving AI model accuracy from 65% to 74%. This directly reduced the time and steep costs associated with early-stage drug discovery.[1]
- Drastic Cost & Energy Reductions - Integrating hardware-accelerated confidential infrastructure allowed the organization to achieve a 1.6X reduction in acquisition costs and a 1.6X reduction in energy consumption per computation compared to standard CPU-only alternatives.[1]
- Massive Operational Efficiency - For large-scale genomic workflows, total energy expenditure dropped from 2.4 GWh to 1.5 GWh, drastically reducing analysis runtime and minimizing the environmental impact of compute-heavy research.[1]

Beyond pharmaceutical development, this secure architecture provides a baseline blueprint for data collaboration across other highly regulated sectors - such as financial services, healthcare, and biometric analytics - where data access limitations stifle technological innovation.

Key Takeaway

For advanced AI initiatives, the limiting factor is no longer algorithm architecture or raw compute capacity, it is secure access to high-quality data.

Confidential Computing addresses this challenge by protecting data not only at rest and in transit, but also during active processing. Combined with hardware-based attestation, it establishes a verifiable foundation of trust that allows multiple institutions to collaborate on AI and analytics without relinquishing control of their most valuable digital assets. As organizations seek to scale distributed AI models, Confidential Computing offers a compliant, practical path to innovation without compromising privacy or commercial security.

References

1. Lab Confidential: Japan Research Keeps Healthcare Data Secure.
Japan Research Keeps Healthcare Data Secure