Leveraging a Zero-Trust Environment to Accelerate AI/ML & Analytic Development

Background

Artificial intelligence (AI), machine learning (ML), and analytic models hold the promise of improving care, reducing unnecessary costs, and optimizing treatment. Unfortunately, most models remain in the early development phase where they are trained on limited data sets, de-identified data, or synthetic data.

As developers move into later development phases, they face an almost insurmountable challenge in accessing personally identifiable and protected health information (PII/PHI) required to understand the model's performance "in the real world" and to demonstrate generalizable performance. The current paradigm of data access is based on sharing and seeing the data. When a data agreement is even possible, it typically takes 12-18 months to complete under clinical trial, patient consent conditions.

Improving Data Security & Enabling Sightless Computing

EscrowAI® is a patent protected[1] privacy enhancing collaboration platform operating in a zero-trust, Trusted Executive Environment within the data steward's secure environment. The platform protects data sovereignty and privacy as well as the intellectual property of the model(s).

EscrowAI provides protections for data steward and model developer:

Data Steward Protections	Model Developer Protections
A project-specific curated data set is encrypted and placed into storage in the Data Steward's secure environment	The model is encrypted and uploaded to EscrowAI where it is placed in a secure container
Encrypted data moves into the confidential computing enclave spun up in the Data Steward's environment	EscrowAI assigns a key to the model container and passes it to the enclave
Data Steward proprietary key protects the data until it recognizes the model's key	The model container is sent to the Data Steward environment where it is pulled into the secure enclave
Once the keys are attested, the data is unencrypted inside the secure enclave while the model computes on the data	A confidential performance report is only sent to the model developer (Unless stipulated otherwise)
PHI never leaves the data steward's environment nor is it ever exposed	Model weights are never shared or seen

[1] US Patents 11,531,904; 1,748,633; 12,001,965; 12,093,423; 12,099,630; 12,111,951 and other patents pending.

EscrowAI Use Cases

EscrowAI's platform supports multiple use cases including (but not limited to):

- Industry and grant sponsored research to train and validate AI/ML solutions.
- Ethical monetization of data (including portals).
- Deploy and monitor AI/ML solutions.
- Privacy enhancing infrastructure to support multi-site, multi-party research.
- Enable compute on data that is jurisdictionally restricted (cannot leave a location).
- AI Assurance: commercial AI/ML model solution testing prior to deployment.

Benefits

- Enables ethical data monetization revenue for data stewards.
- Reduces the risk of data breaches and resulting sanctions.
- Provides data and IP protection at rest, in transit, and during compute.
- Promotes precision breakthroughs due to enabling confidential computing on PII/PHI.
- Minimizes the administrative overhead and cost of approvals and contracting.
- Accelerates the approvals/contracting process thereby accelerating time to market.
- Enables data stewards to minimize the time and risks associated with new AI/ML solutions prior to deployment.
- Complies with data sharing requirements for funding and publication as well as the Presidential Executive Order to Improve Cyber Security.

A Customer Story

Novartis Biome contracted with BeeKeeperAI to assist in validating a proprietary algorithm designed to assist in identifying pediatric patients with a rare disease. Historically, the PHI data for the patient population was impossible to access due to the inability to de-identify the data. In addition, Novartis wanted to protect the intellectual property of its algorithm.

With EscrowAI, Novartis computed on PHI containing a gold standard data subset of less than 30 patients with the rare disease diagnosis. Through its iterative experimentation on EscrowAI Novartis was able to sightlessly improve the performance of its model. As the Novartis Biome recently stated, "The impossible is now possible."

Learn More

BeeKeeperAI is a spin-out of the University of California, San Francisco's Center for Digital Health Innovation where the founding team learned first-hand the challenges facing model owners and data stewards seeking to advance innovation while optimizing data sovereignty, privacy, and security.

Click for an overview of EscrowAI. Click for the Azure Marketplace listing.