In a classic centralized setup, all data used for training is transferred to a central location. Yet, this is often impossible.

“"We want to offer AI applications like predictive maintenance or clinical decision support to our customers. Yet hospitals cannot share their sensitive patient data with us. It takes years to get such a specific patient consent.”

CDO of large MedTech provider

Sharing or centralizing data can be impossible or dangerous

- IP protection of data and AI model
- Data protection regulation
- Distrust in other parties
How Federated Machine Learning works

Instead of centralizing huge amounts of training datasets for machine learning purposes, we bring the AI models to multiple local and secured datasets instead.

Data scientists can analyze distributed data in a secure and privacy preserving manner.

Data Owners can safely collaborate and commercialize their data assets without compromising data privacy.
Our touchpoints with IP

IP rights are important for us under different aspects:

- untrained AI model
- proprietary datasets
- local trained AI model
- global trained AI model
- our proprietary software

Possible IP implications
We offer a technical solution to a legal problem

If IP sensitive information is not secured and preserved, private sharing that data is impossible or dangerous.

Our solution protects data in a technical way, irrespective of the reason for it being sensitive.

- Datasets of data owners reside locally in isolated secure environments
- Privacy preserving technologies make sure that trained AI models do not leak data
- Only authorized party or parties receive the trained AI model
- Each individual isolated environment is locked during model training, no one has access to the proprietary AI model
Apheris is on a mission to fundamentally change how organizations collaborate securely and extract value from data

We are an interdisciplinary team of technical and scientific experts (60% with a PhD) and have raised more than USD 4M from leading European and US investors.