

Privacy Compliant Patient Monitoring

Industry: Healthcare & MedTech

Sensitive patient data cannot leave local servers without proper HIPAA/GDPR compliance. Federated Learning to the rescue.

The Problem

A MedTech startup built a wearable for cardiac arrhythmia detection but couldn't scale because hospitals refused to let sensitive patient ECG data leave their local servers for model training (HIPAA/GDPR risk).

Solution

The "Hard Tech" Solution: Klyff deployed a **Federated Learning architecture**. The global AI model was sent to 50 different hospital edge servers. The models learned from local data, and only the "mathematical weights" (not the patient data) were sent back to the Klyff orchestrator to improve the master algorithm.

1. Hardware

- **Edge Node:** NVIDIA Jetson Orin Nano or Google Coral Dev Board (using the Edge TPU).
- **Edge Server (The Aggregator):** Advantech AIR-150 or an Intel NUC running OpenVINO to process encrypted model weights.

2. Software

- **Federated Framework:** Flower (flower.ai) or OpenMined (PySyft) for secure, decentralized training.
- **Machine Learning:** LiteRT (the new name for TensorFlow Lite as of 2025).
- **Communication:** gRPC with TLS encryption to handle the secure exchange of model weights between Klyff and the hospital nodes.

Results



Through federated learning, Klyff was able to orchestrate across fragmented networks

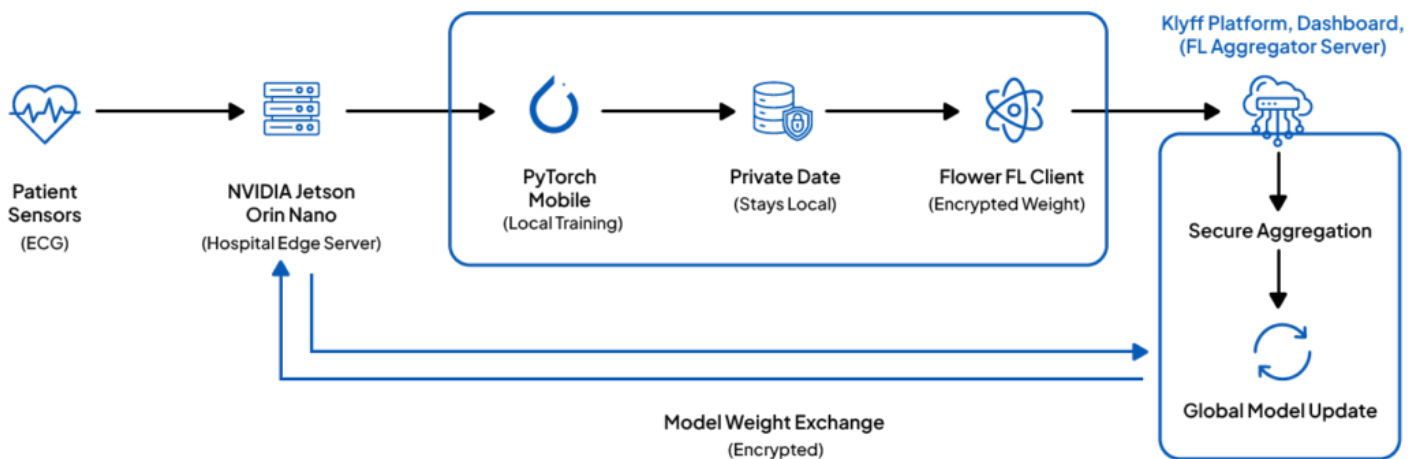


Complete HIPAA / GDPR compliance



A 15% increase in diagnostic accuracy across diverse populations without moving a single byte of PII (Personally Identifiable Information).

Solution Flow



Let us help you with Privacy & Federated Learning

✉ sales@klyff.com

🌐 www.klyff.com