

Federated & Privacy Preserving Biomedical ML — Hands-on

Design and deploy privacy-first ML workflows across hospitals, labs, and devices. This module covers the federated learning (FL) stack—algorithms, systems, and privacy tech—so you can collaborate on biomedical models without centralizing sensitive data. You will implement secure training, evaluate privacy/utility trade-offs, and generate compliance-ready artifacts.

Federated & Privacy Preserving Biomedical ML

[Help Desk](#) · [WhatsApp](#)

Session Index

[Session 1 — FL Foundations & System Design](#) [Session 2 — Algorithms, Non-IID & Personalization](#)
[Session 3 — Privacy Tech: DP, Secure Agg, HE/MPC](#) [Session 4 — Mini Capstone: Secure FL Pipeline](#)

Session 1

Fee: Rs 14,400 [Apply Now](#)

FL Foundations & System Design

Federated learning settings & topologies

[cross-silo / cross-device](#) [horizontal / vertical / hybrid](#) [orchestration & messaging](#)

Frameworks & tooling

[TensorFlow Federated](#) [Flower / FedML](#) [PySyft](#)

Systems concerns

client reliability & dropout communication efficiency
monitoring & logging

Session 2

Fee: Rs 19,800 Apply Now

Algorithms, Non-IID & Personalization

Optimization and aggregators

FedAvg / FedProx FedAdam / Scaffold adaptive client
selection

Non-IID, drift & heterogeneity

skewed labels/features domain shifts robust metrics

Personalization strategies

fine-tuning/partial layers meta-learning multi-task
heads

Session 3

Fee: Rs 25,600 Apply Now

Privacy Tech: DP, Secure Agg, HE/MPC

Differential Privacy (DP) in training

DP-SGD / clipping & noise ϵ , δ & privacy budgets
utility trade-offs

Secure aggregation & encryption

secure agg protocols homomorphic encryption MPC
basics

Governance & compliance aware design*

consent & audit logs data minimization HIPAA/GDPR
context

*This training is educational and not legal advice.

Session 4

Fee: Rs 32,000 Apply Now

Mini Capstone: Secure FL Pipeline

Orchestrate an end-to-end FL experiment (cross-silo)

Theory + Practical

Add privacy & security layers

DP-SGD **secure aggregation** **encryption keys**

Deliverables: code, privacy report & model card

notebook/script **€ accounting** **PDF/HTML**