atlanTTic
Universidade de Vigo

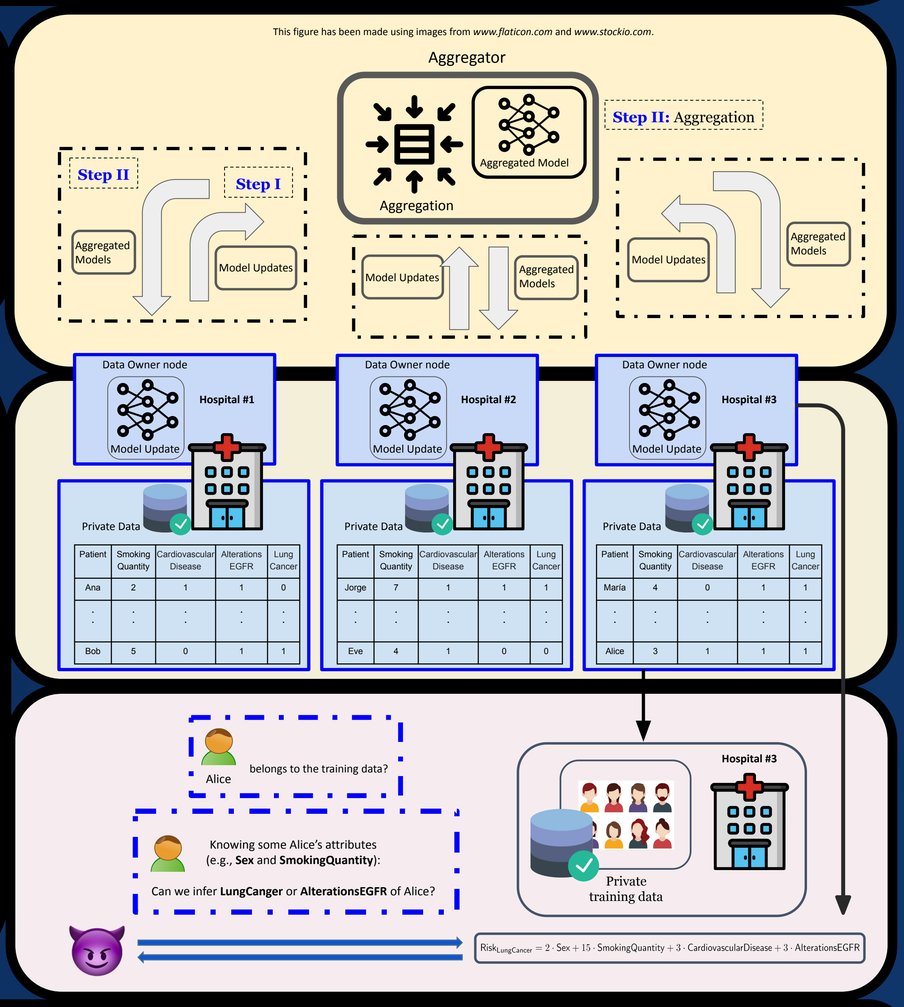
Privacy-Enhanced Federated Learning for Hospital Collaboration

Alberto Pedrouzo-Ulloa · apedrouzo@gts.uvigo.es

Presented at Galicia Biodays 2026, Vigo, 6-7 May 2026

Why Federated Learning for Hospital Collaboration?

- Single hospitals rarely provide enough data for robust biomedical AI.
- FL enables cross-hospital collaboration while **keeping patient data on-site**.
- Hospitals train a shared model by exchanging model updates instead of raw records.



Privacy risks remain in FL:

- Exchanged model **updates may still leak information** about patients.
- Attackers can exploit updates to infer whether a record was used for training (membership inference) or to predict hidden patient attributes (attribute inference).

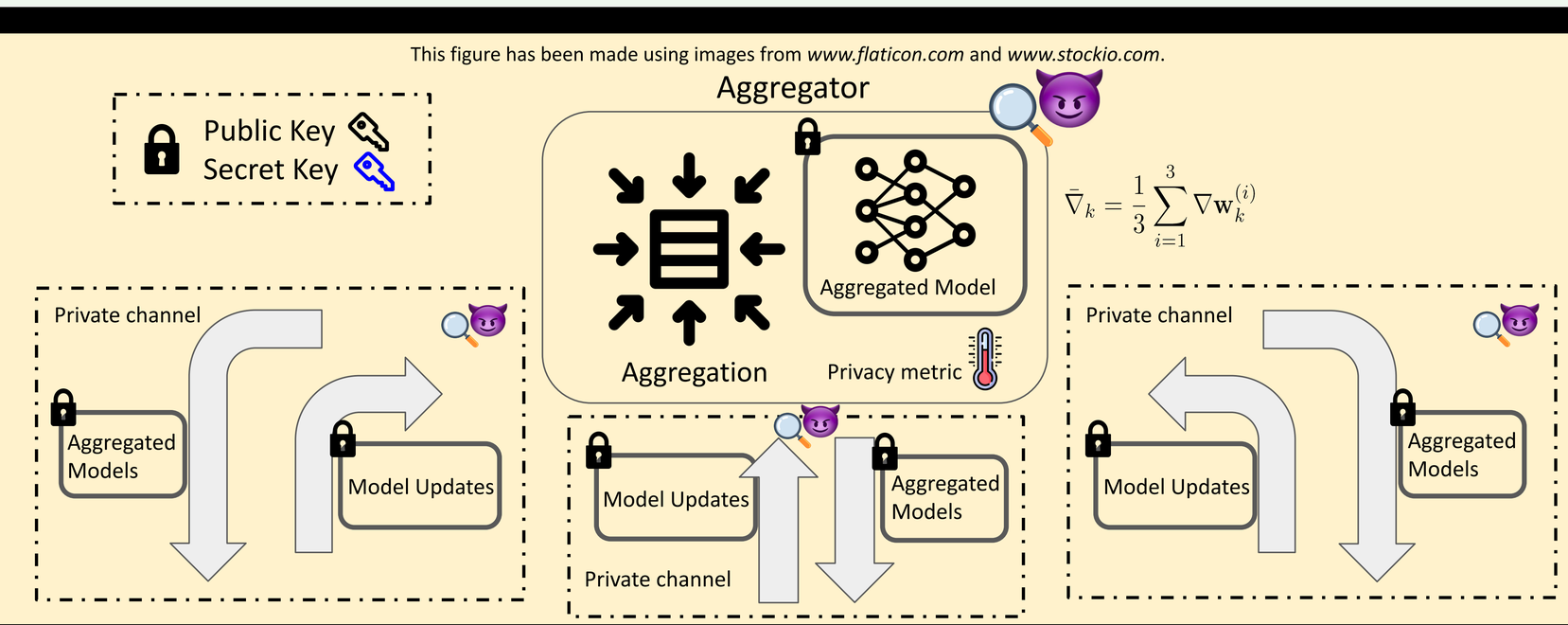
Membership inference: Even 1-bit leakage can matter

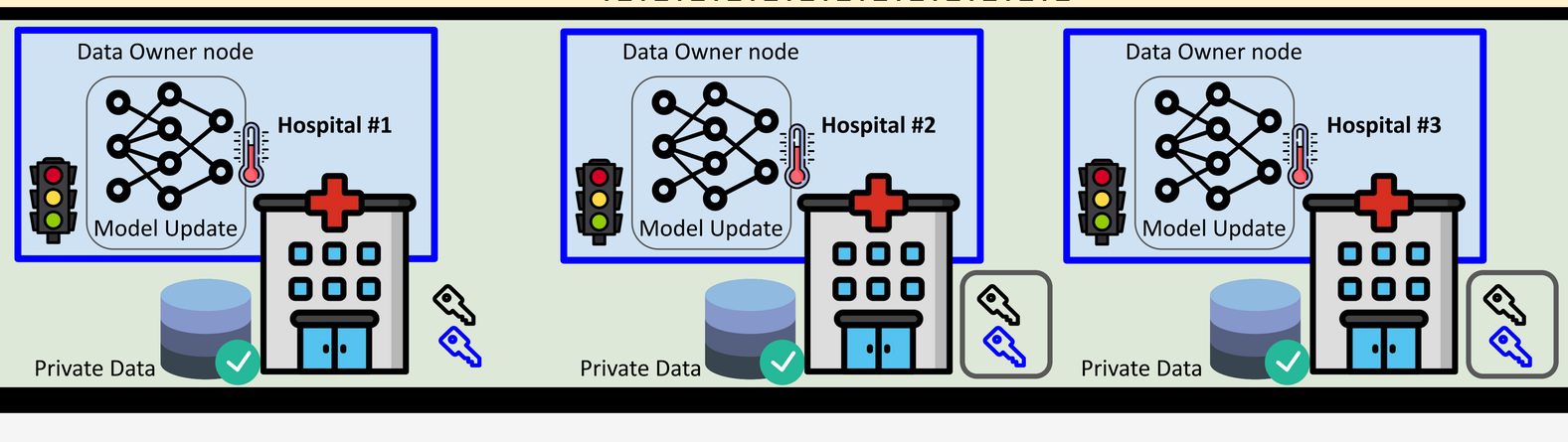
Source: *https://www.cancer.gov/about-cancer/causes-prevention/risk/age*.

- General cancer risk 🧍:
  - 350 per 100000 people (aged 45 - 49)
- "Cancer risk" knowing that 🧍 is contained in the training data:
  - 1 per 2 people

We propose privacy-enhanced FL:

- **Homomorphic-encrypted secure aggregation:** the aggregator processes encrypted updates without accessing individual updates.
- **Privacy risk measurement:** hospitals evaluate each update before sharing it to detect potential leakage of sensitive information.





Some conclusions:

- **Keeping patient data on-site is not enough**: FL must also protect model updates and measure residual privacy leakage.
- Combining **homomorphic-encrypted secure aggregation** with **privacy risk measurement** enables safer and more trustworthy hospital collaboration for biomedical research.

XUNTA DE GALICIA
Rede CIGUS
Centros de investigación do Sistema Universitario de Galicia
Cofinanciado pola Unión Europea
Fondos Europeos