Privacy-preserving federated learning for hospital collaboration

Galicia Biodays 2026

Auditorio Mar de Vigo
6-7 May 2026, Galicia, Spain

Presentation at Sala BioInternational
Thursday, *7 May 2026*

Alberto Pedrouzo-Ulloa
apedrouzo@gts.uvigo.es

Outline



- Introduction
- Federated Learning
- Privacy threats
- Privacy-enhanced FL
- Conclusions

TRUMPET Funded by the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038



Introduction

When AI meets medical data: a privacy love story in Paris

TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038



Introduction

When AI meets medical data: a privacy love story in ~~Paris~~ Vigo

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

High-level Workflow in Machine Learning

Gather enough data:

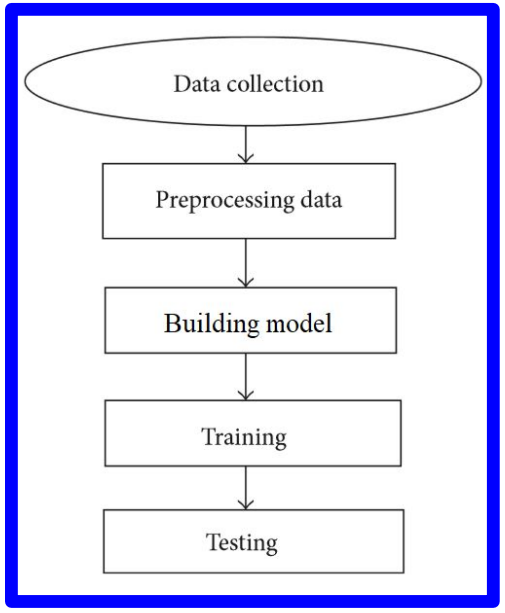
- *Data collection*
  - *Gather relevant data*
- *Preprocessing data*
  - *Clean and prepare the data for analysis*

Train a model:

- *Build an ML model (Choose an adequate model, model training, hyperparameter tuning, evaluate the model, etc)*

Deploy the model:

- *Use the trained model for your application (e.g., query an input sample for a prediction or classification task)*

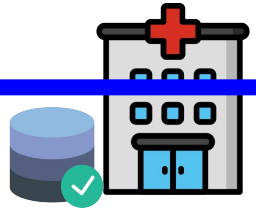


TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

High-level Workflow in Machine Learning

Gather enough data:

- *Data collection*
  - *Gather relevant data*
- *Preprocessing data*
  - *Clean and prepare the data for analysis*

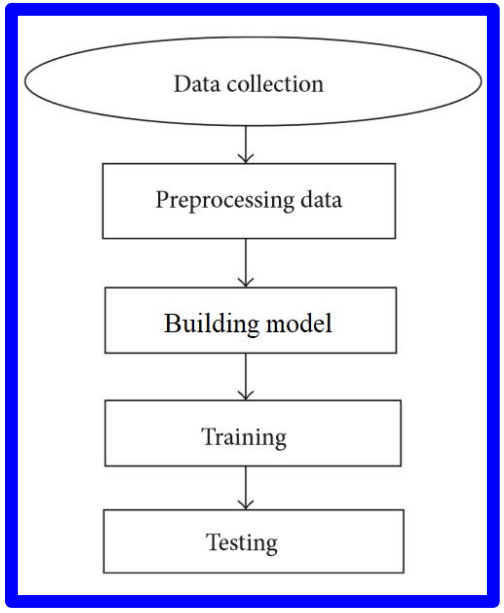


Train a model:

- *Build an ML model (Choose an adequate model, model training, hyperparameter tuning, evaluate the model, etc)*

Deploy the model:

- *Use the trained model for your application (e.g., query an input sample for a prediction or classification task)*

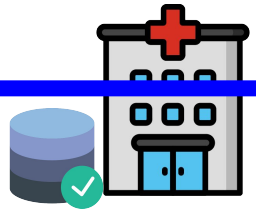


TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

High-level Workflow in Machine L

Gather enough data:

- *Data collection*
  - *Gather relevant data*
- *Preprocessing data*
  - *Clean and prepare the data for analysis*



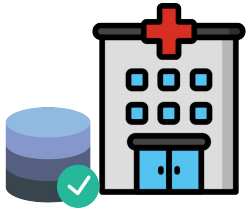
TRUMPET

gradiant · Arteevo · Inria · atlanTTic research center for Telecommunication Technologies Universidad de Vigo · Servizio Sanitario Regionale Emilia-Romagna, Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori" – Istituto di Ricovero e Cura a Carattere Scientifico · IRST Istituto Romagnolo per lo Studio dei Tumori Dino Amadori · TIMELEX · CHU de Liège · cea · TECHNOVATIVE SOLUTIONS · Republic of Türkiye Ministry of Health

A first meeting with TRUMPET:

- European project on privacy-enhanced AI studies using multi-site cancer data.
- Clinical data from multiple healthcare partners:
  - IRST — IRCCS Istituto Scientifico Romagnolo per lo Studio e la Cura dei Tumori.
  - CHU de Liège — Centre Hospitalier Universitaire de Liège.
  - MoH Türkiye — Turkish Ministry of Health.
- Data scope: cancer patients, treatments, outcomes, and adverse effects.

High-level Workflow in Machine Learning

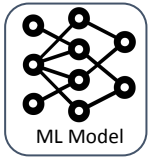


Gather enough data:

- *Data collection*
  - *Gather relevant data*
- *Preprocessing data*
  - *Clean and prepare the data for analysis*

Train a model:

- *Build an ML model (Choose an adequate model, model training, hyperparameter tuning, evaluate the model, etc)*



Deploy the model:

- *Use the trained model for your application (e.g., query an input sample for a prediction or classification task)*

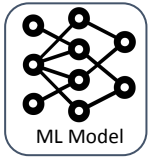
TRUMPET Funded by the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

High-level Workflow in Machine Learning

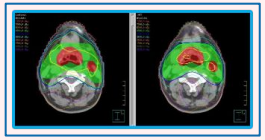
Train a model:

- *Build an ML model (Choose an adequate model, model training, hyperparameter tuning, evaluate the model, etc)*



Three target AI models:

- **Immunotherapy response prediction in metastatic Non-Small Cell Lung Cancer (NSCLC):**
  - Train a model capable of predicting patient prognosis using multiple markers.



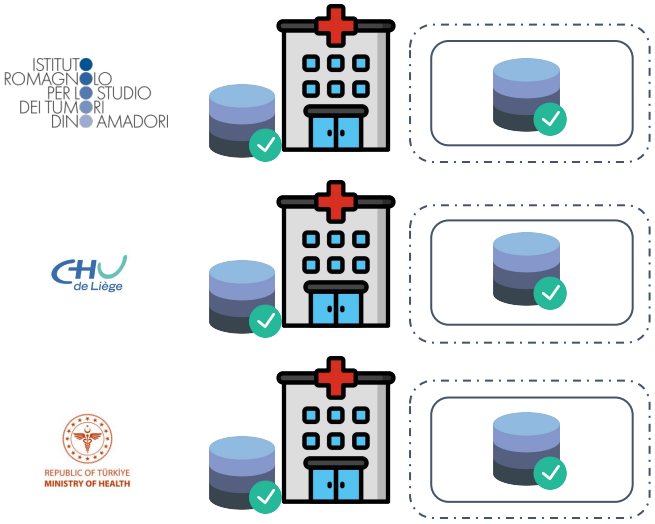
- **Late side effects prediction in Head and Neck Cancer (HNC) radiotherapy:**
  - Train a model capable of predicting side effects in HNC patients treated with IMRT.



- **Survival prediction for Stereotactic Body Radiotherapy (SBRT) eligibility:**
  - Train a model capable of predicting six-month survival probability.

What if data comes from different sources?

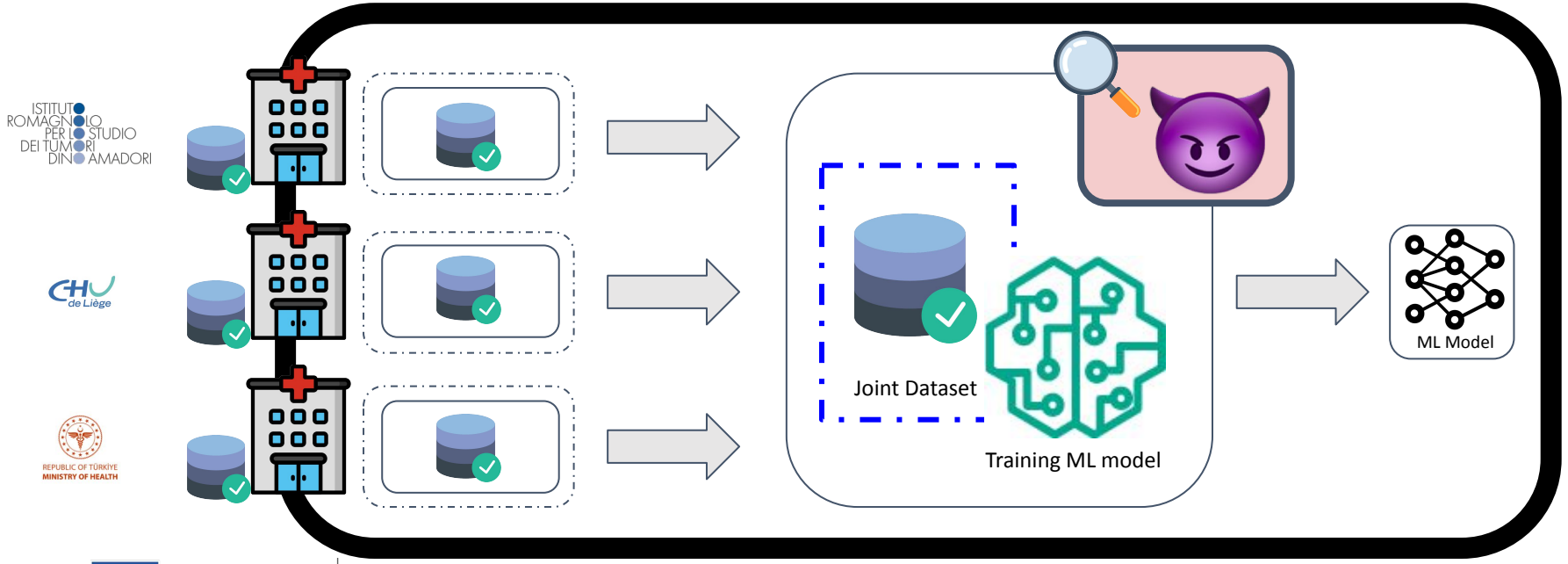
- **All local data must be sent to a trusted party**
  - Then, the training can be done as usual!



Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

What if data comes from different sources?

- **All local data must be sent to a trusted party**
  - Then, the training can be done as usual!



TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

The guest list must be private: sensitive patient records

Patient profile

Clinical status

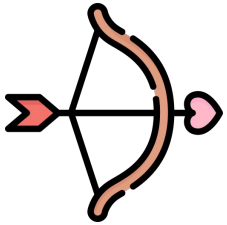
Cancer-specific information

Treatment history

Outcomes and adverse events

- ***Demographic patient information:***
  - *e.g., age, sex, smoking quantity, etc.*
- ***Social and psychological patient status:***
  - *e.g., living place, home type, marital status, occupation, etc.*
- ***Laboratory testing parameters:***
  - *neutrophils, lymphocyte, eosinophils, monocyte, basophils, etc.*
- ***Certain comorbidities:***
  - *e.g., diabetes, cardiovascular disease, autoimmune disease, etc.*
- ***Prognostic indicators:***
  - *estimated survival by doctor, presence of metastases, etc.*
- ***Pathological markers:***
  - *e.g., PDL1, ALK, ROS1, etc.*
- ***Presence of relevant gene alterations:***
  - *e.g., EGFR, KRAS, MET, LKB1, etc are relevant in the case of Lung Cancer.*
- ***Tumor characteristics:***
  - *e.g., tumor size, type of tumor, tumor stage, etc.*
- ***Treatment history:***
  - *e.g., types of previous treatments (surgery, radiotherapy, chemotherapy, immunotherapy), treatment start/end date, reason for end of therapy, etc.*
- ***Disease progression:***
  - *presence or absence of disease progression, date of disease progression, etc.*
- ***Treatment-related adverse effects:***
  - *list of side-effects caused by applied treatments, severity of side effects, etc.*

Funded by the European Union







Federated Learning

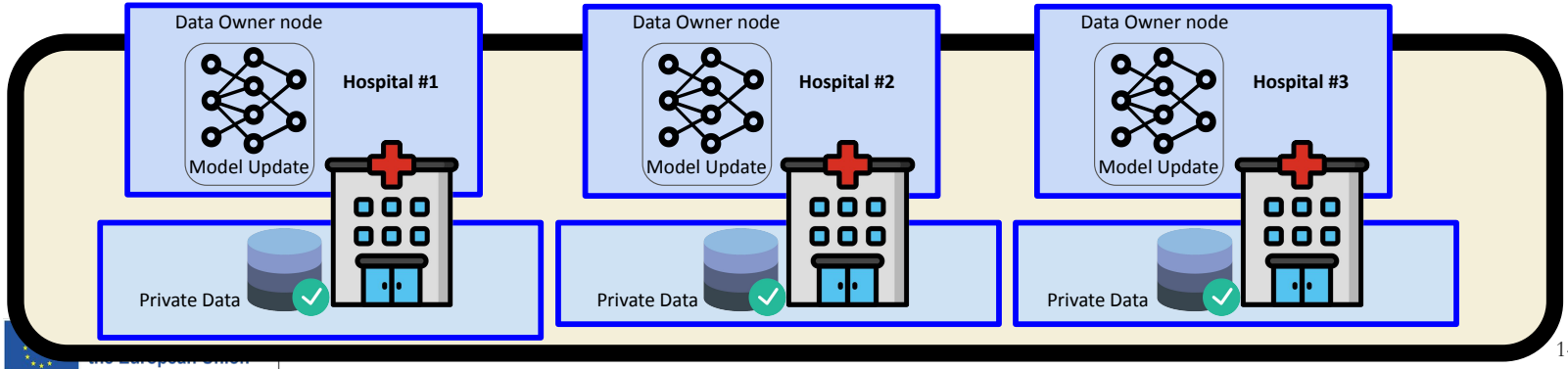
A match made in AI heaven: Hospital collaboration and federated learning

TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

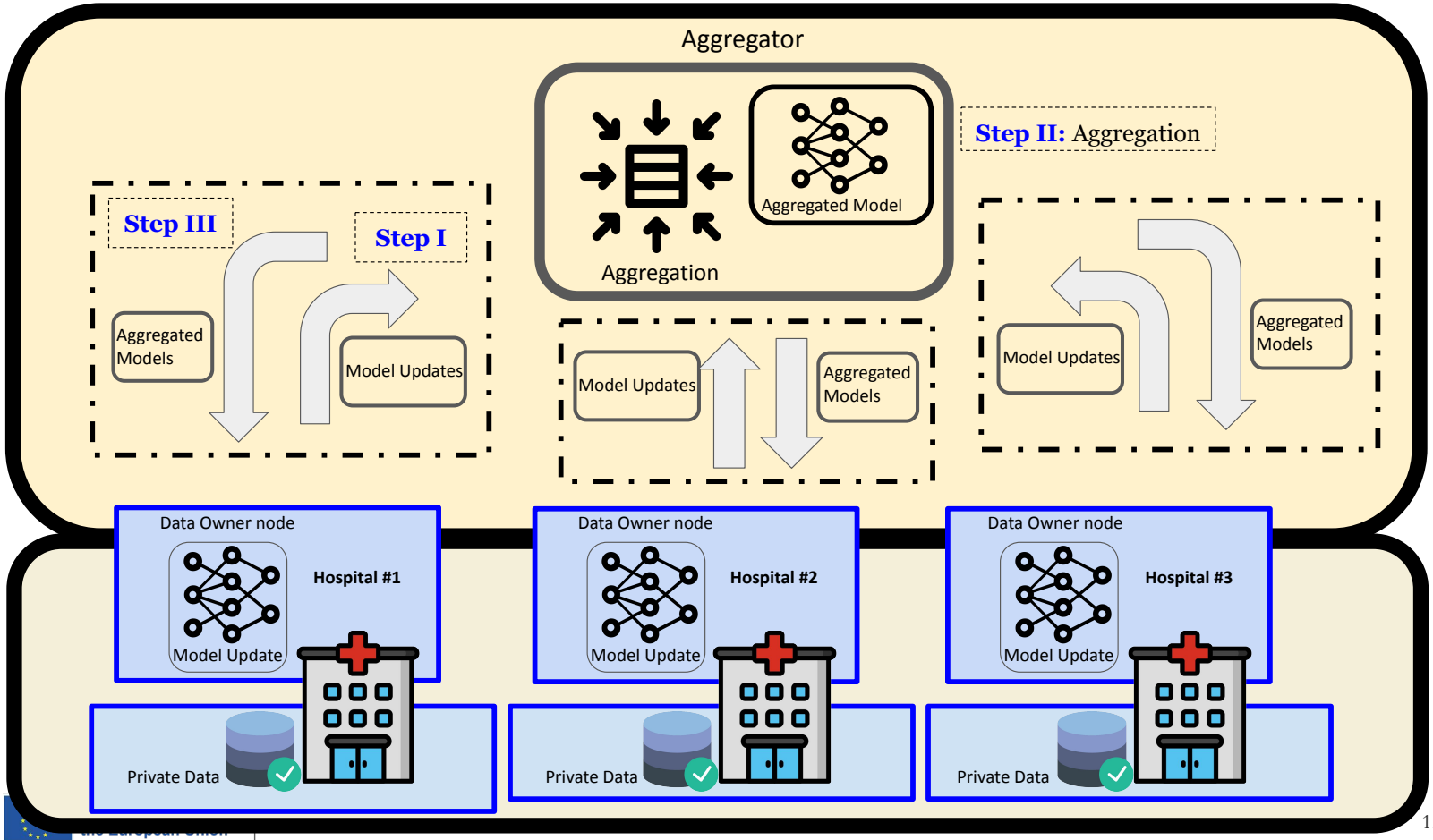
Our FL scenario

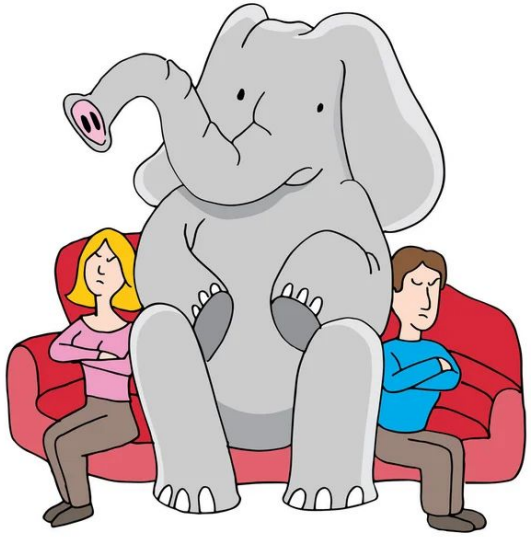
Why Federated Learning for Hospital Collaboration?

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



Our FL scenario





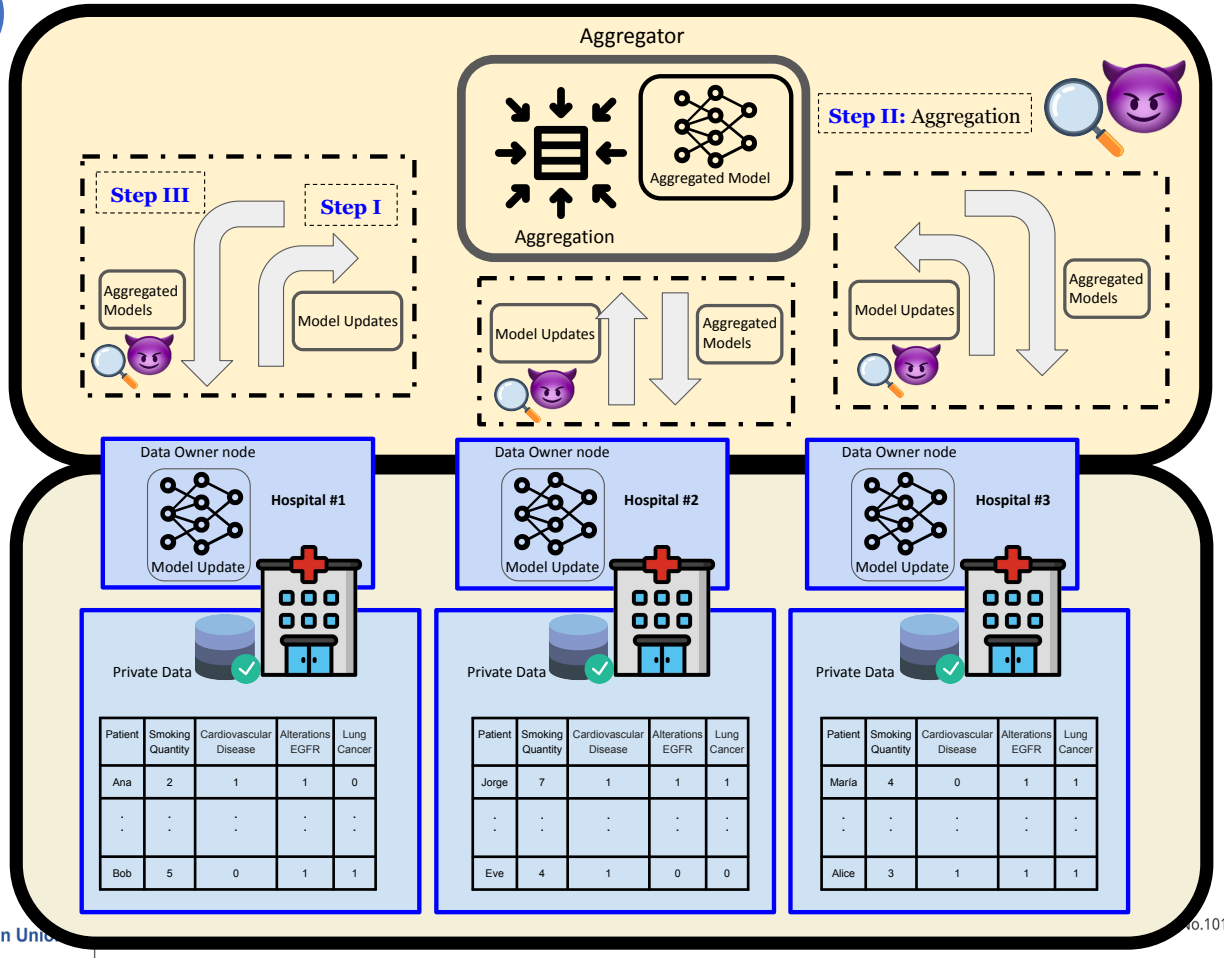
Privacy threats remain in FL

A new Hope or… an elephant in the room?

Funded by the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

PRIVACY LEAKAGE: TROUBLE IN THE PARADISE?



Patient	Smoking Quantity	Cardiovascular Disease	Alterations EGFR	Lung Cancer
Ana	2	1	1	0
...	...	...	...	...
Bob	5	0	1	1

Patient	Smoking Quantity	Cardiovascular Disease	Alterations EGFR	Lung Cancer
Jorge	7	1	1	1
...	...	...	...	...
Eve	4	1	0	0

Patient	Smoking Quantity	Cardiovascular Disease	Alterations EGFR	Lung Cancer
María	4	0	1	1
...	...	...	...	...
Alice	3	1	1	1

Funded by the European Union
o.101070038

SOME PRIVACY RISKS: SPEAK NOW OR FOREVER HOLD YOUR PEACE

- Exchanged **model updates may still leak information** about patients.
- Recent studies have shown it is **feasible to extract private information from 👤's records** based on the **exchanged updates during FL training**.

$$\text{Risk}_{\text{LungCancer}} = 2 \cdot \text{Sex} + 15 \cdot \text{SmokingQuantity} + 3 \cdot \text{CardiovascularDisease} + 3 \cdot \text{AlterationsEGFR}$$

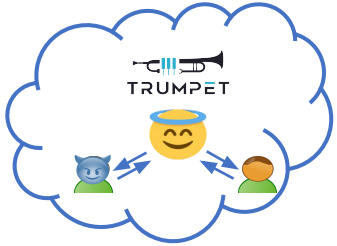
Model Update

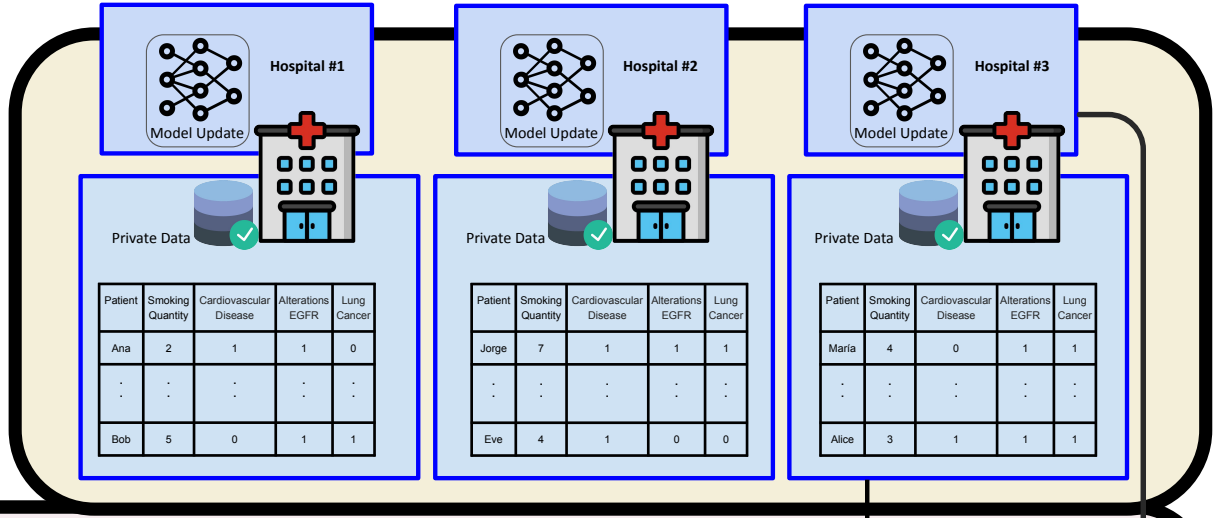


- Different attacks can be implemented **depending on the knowledge the adversary** has about 👤's record.

TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

PRIVACY LEAKAGE: A TOY EXAMPLE



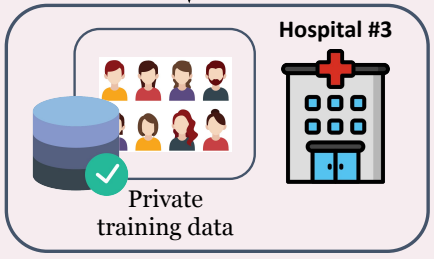


An example:
Inference attacks

Alice belongs to the training data?

Knowing some Alice's attributes (e.g., **Sex** and **SmokingQuantity**):
Can we infer **LungCancer** or **AlterationsEGFR** of Alice?

Real use cases	Adversary membership accuracy
NSCLC	70%
HNC	53%
SBRT	85%



$$\text{Risk}_{\text{LungCancer}} = 2 \cdot \text{Sex} + 15 \cdot \text{SmokingQuantity} + 3 \cdot \text{CardiovascularDisease} + 3 \cdot \text{AlterationsEGFR}$$

MEMBERSHIP INFERENCE: TELL ME WHO YOU GO WITH, AND I'LL TELL YOU WHO YOU ARE

- **Membership inference:**
  - General cancer risk  : 350 per 100000 people (aged 45 - 49)

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

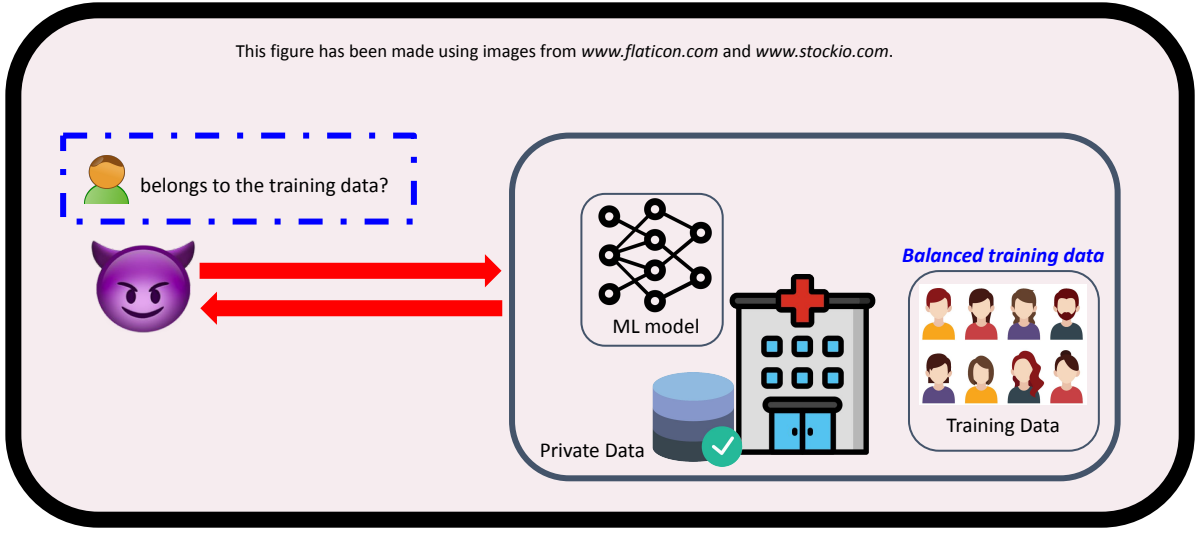
TRUMPET Funded by the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

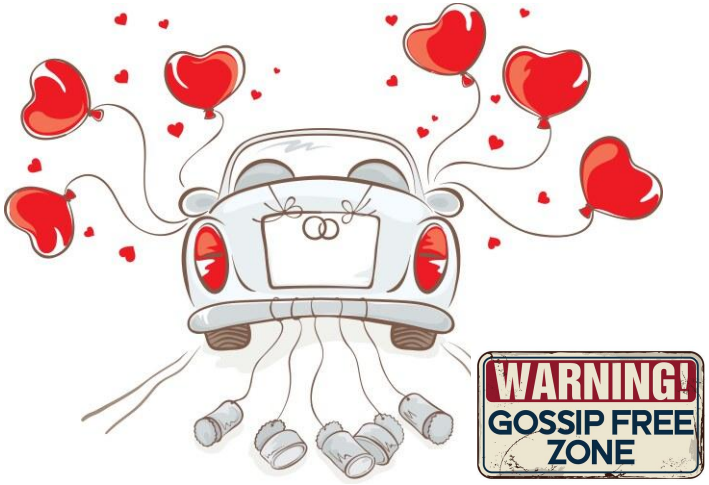
MEMBERSHIP INFERENCE: TELL ME WHO YOU GO WITH, AND I'LL TELL YOU WHO YOU ARE

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

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



Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038



Privacy-enhanced FL

Married life: They lived happily ever after… with a prenuptial agreement

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

What do we propose?

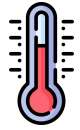
Privacy-enhanced FL relies on two main building blocks:

- **Homomorphically encrypted secure aggregation:**
  - the aggregator *processes encrypted updates* without accessing individual updates.

- **Privacy risk measurement:**
  - hospitals *estimate whether a model update may leak sensitive patient information* before sharing it.



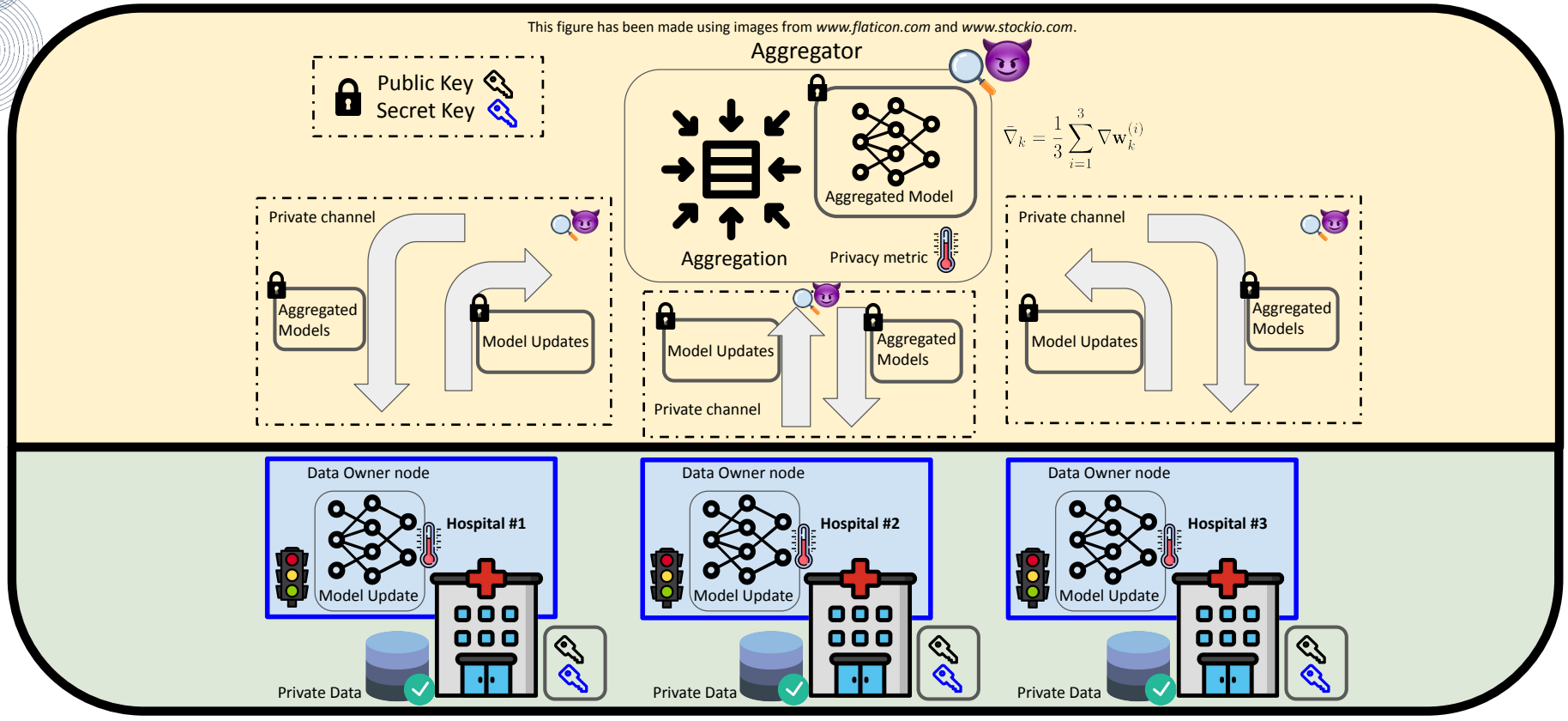




Privacy metric

TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

How does this work in practice?



TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038



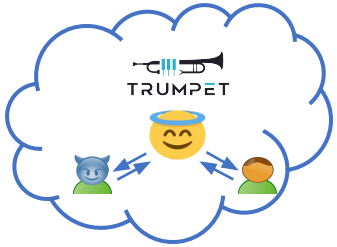
Conclusions

The take-home message: love is not enough

Funded by the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

Conclusions



- **Medical AI needs collaboration**, but sensitive patient records should not be centralized.
- **Federated Learning helps** by keeping raw data on-site and exchanging only model updates.
- **FL is not enough:** model updates may still leak sensitive information.
- **Privacy-enhanced FL adds two safeguards:** encrypted secure aggregation and privacy risk measurement.
- **TRUMPET showcases these technologies** for safer hospital collaboration in biomedical research.

TRUMPET
Funded by the European Union
Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

atlanTTic
research center
for Telecommunication Technologies
Universidade Vigo

Funded by
the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

Thanks for your attention!

