



Oliver Kohlbacher

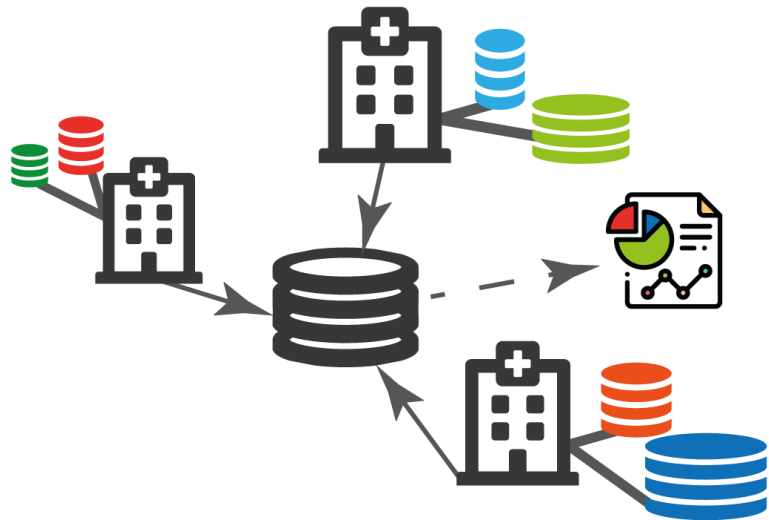
July 01, 2026

MIRACUM-DIFUTURE Symposium 2026, Mannheim

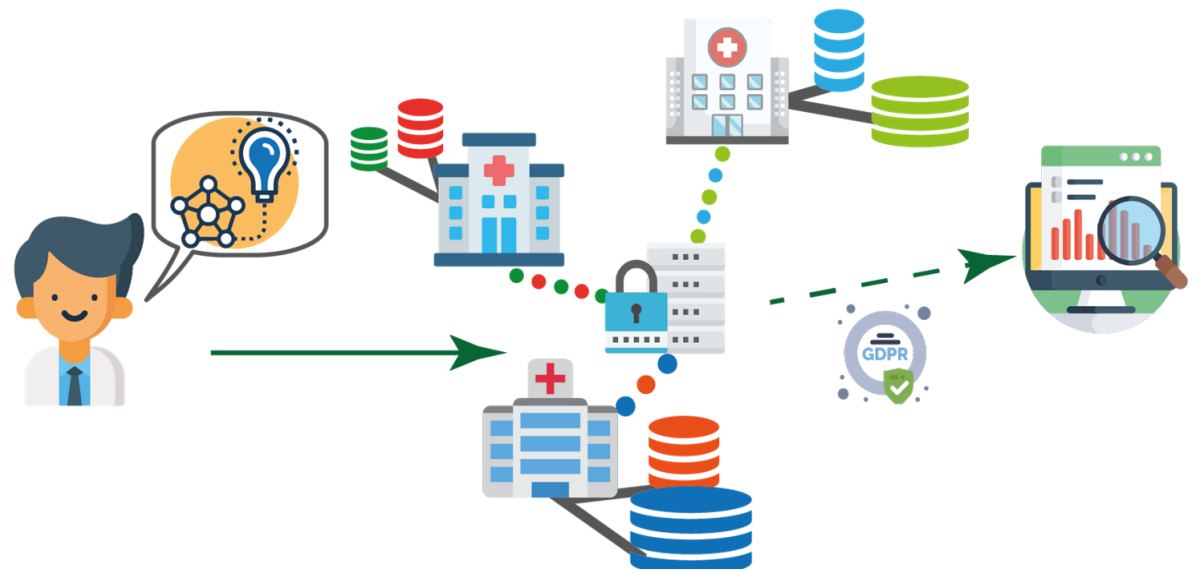
General Idea

***Data** stays under local control by hospitals (nodes). Analyses (containers) are distributed by the hub and globally **aggregate only results/ models**.*

„Code to Data“ Paradigm



Central analysis



Federated analysis

PrivateAIM & the FLAME Platform

Federated Learning and Analytics in Medicine



KEY IDEAS

- 1 Major scientific contributions**
Federated ML methods · privacy guarantees · real-world platform
- 2 One platform across the MII**
Deploy these ideas consistently across all MII sites
- 3 Enabling further use cases**
Support other (clinical) use cases within the MII

PLATFORM HIGHLIGHTS

-  **Open-source platform**
Complex medical data analysis
-  **Secure & compliant**
Safeguards data privacy
-  **New methods for federated learning**
Concepts for federated analytics tested on platform



With funding from the:



Unique Selling Points of the Platform

- FLAME has been designed with the **MII infrastructure** and **large-volume data** in mind
 - Direct connection to FHIR server (after project-specific slicing)
 - Image data and omics data included on S3 server – referenced in FHIR server
 - Can integrate additional external (e.g., CSV) data
 - Integration with FDPG (proposals, identity management)
- In contrast to DataSHIELD
 - No mapping to other representations (OPAL)
 - Ability to deal with large-scale data
 - Flexible integration of complex (bioinformatics, image processing) pipelines



With funding from the:



FLAME Security

✓ Software dependencies

Approved master images · CVE scans



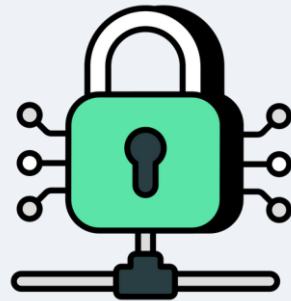
✓ Analysis & project approval

Manually approved & initiated by each site



✓ Encryption

SSL/TLS · ECDH / symmetric-key encryption



✓ Authorization & authentication

All flows protected & controlled



FLAME Security

Maturity model for integrating Privacy-Enhancing Technologies (PETs) in FLAME



Analysis-based

PETs in custom analysis code. No enforcement or audit — full trust in the analyst



Library-based

PETs via FLAME-SDK or libraries.
Transparent & reusable



System-based

PETs enforced by the platform (API & policies)
Strong guarantees, auditable, minimal trust.

Increasing enforcement, auditability & guarantees — decreasing trust in analysis code

FLAME Privacy

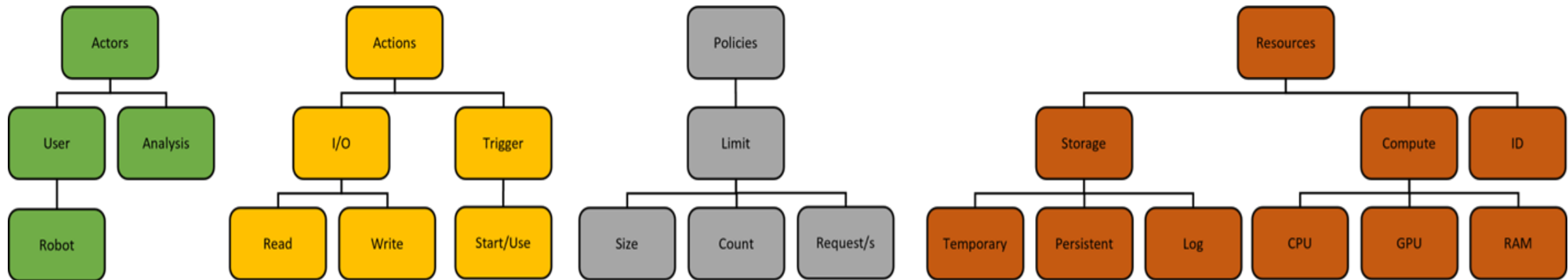
- **Goal** is to develop a framework that can quantify and manage privacy risks for datasets and analysis within the FLAME platform
- **Core idea:** Use the Risk Assessment Application (RAA) to support analysts and data stewards by estimating risk exposure of a dataset or analysis request before execution
- **Aim** is to keep risk exposure below acceptable thresholds
- Different levels of PET (Privacy Enhancing Technology) integration: from analyst-controlled to fully system-enforced protection



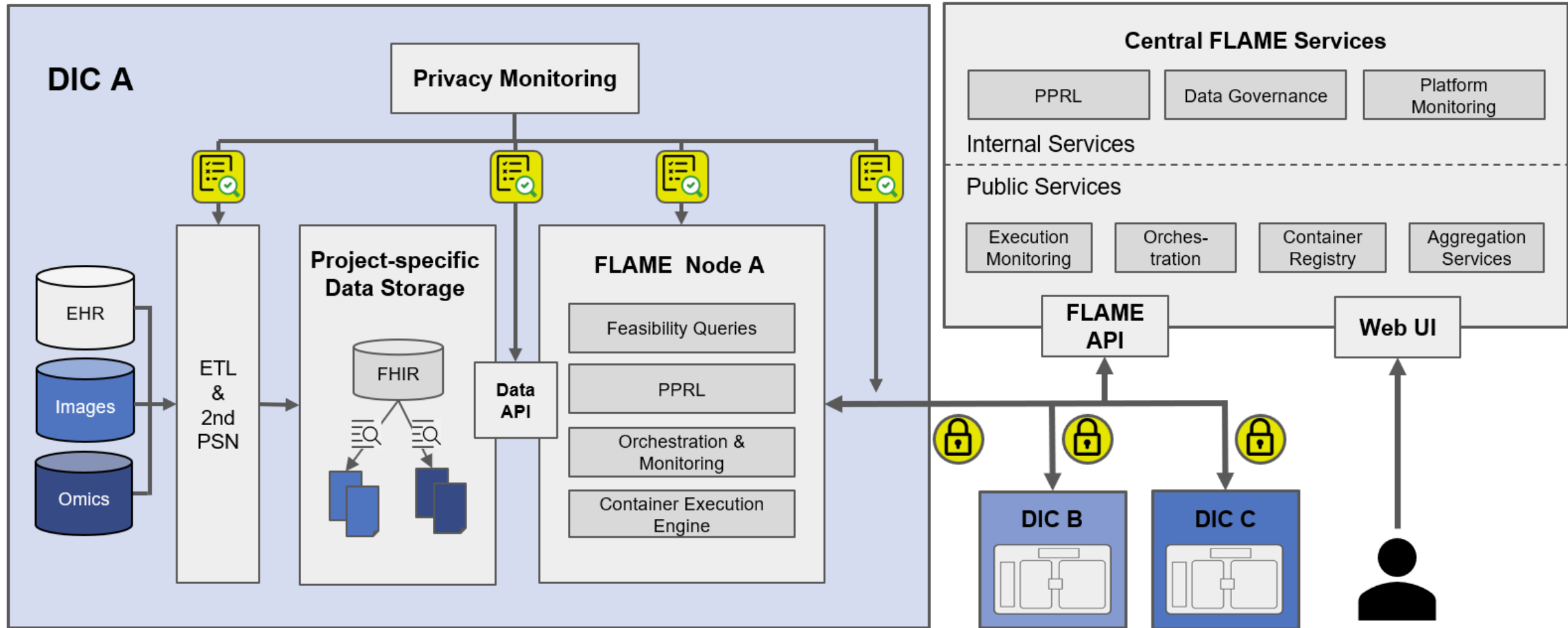
Permissions & Policies

Every permission in FLAME is a combination of **five configurable components** — set individually per node.

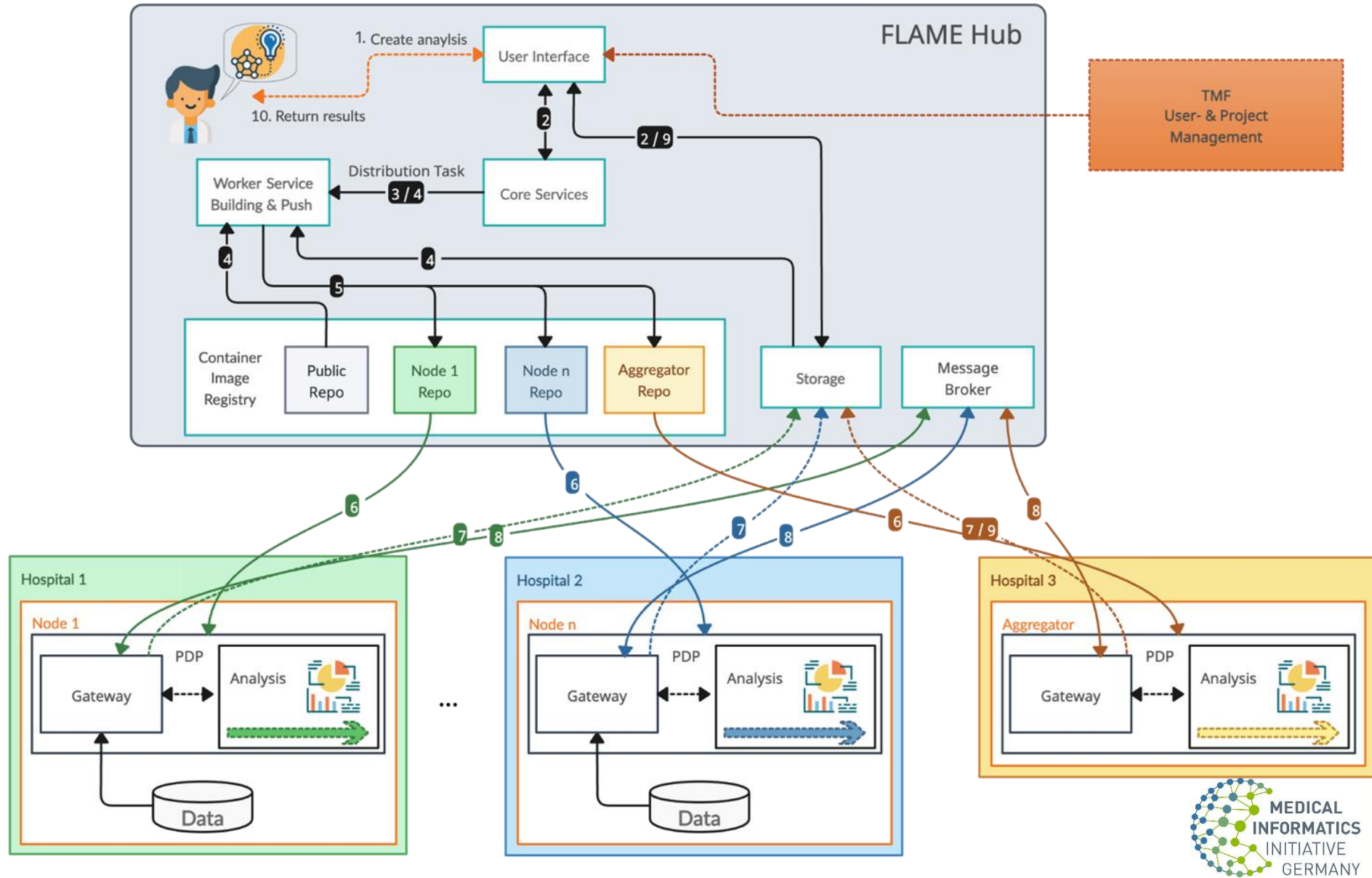
Example: the analysis **[Actor]** writes **[Action]** max 5× **[Policy]** into the storage **[Resource]** of the aggregator **[Context]**.



The FLAME Platform



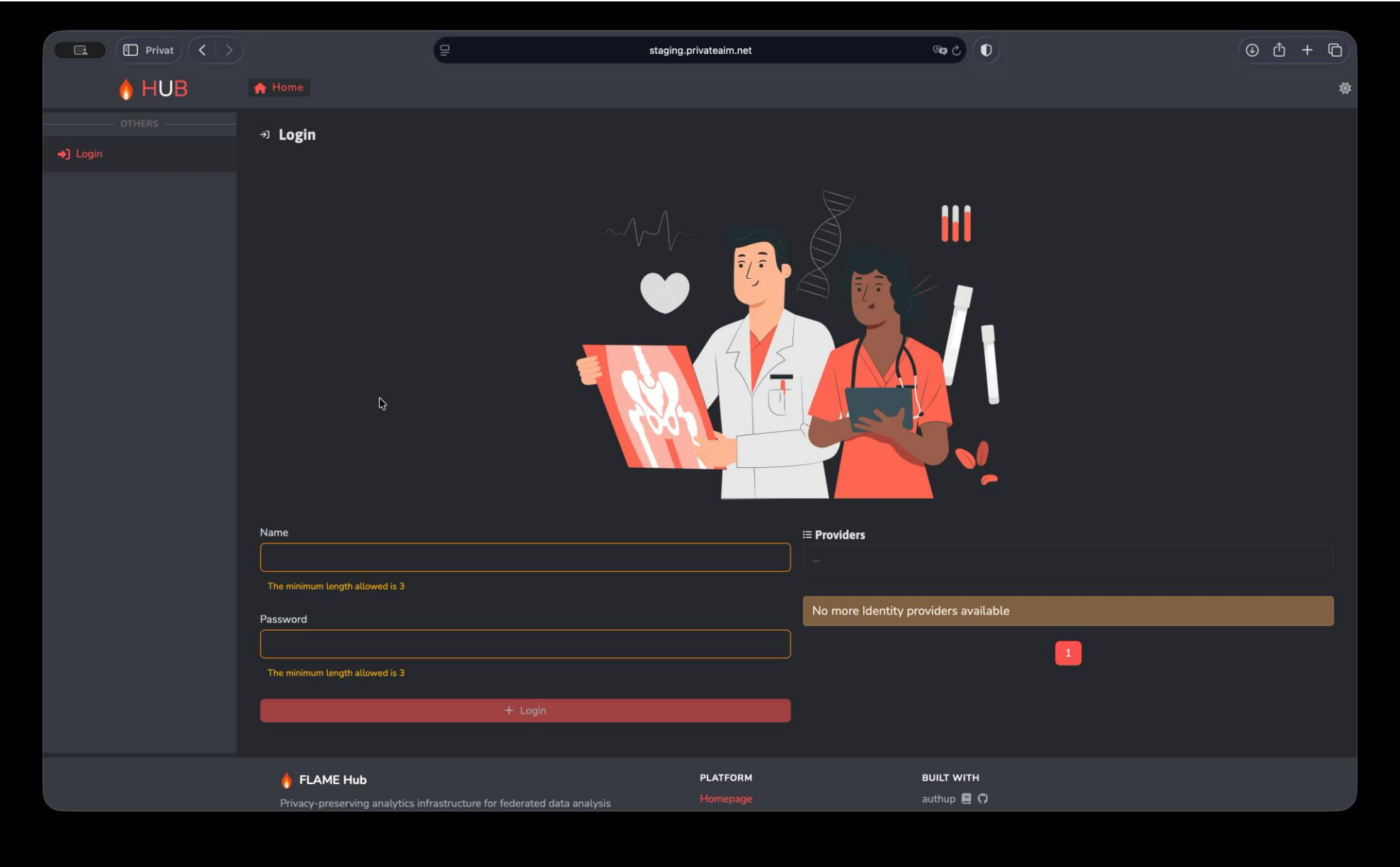
Overview of the Analysis Process



With funding from the:



FLAME Analysis Submission



FLAME Analysis Execution

master

Info

Projects

Analyses

OTHERS

Settings

staging.privateaim.net

Marius Herr

HomeAdmin

Analysis Demo Symposium

OverviewNodesCodeImageResultsSettings

Configuration100%

Build100%

3. Distribution100%

4. Execution99%

Logs

1 info Pushed images9 minutes ago

2 info Pushing images10 minutes ago

3 info Tagged images10 minutes ago

4 info Tagging images10 minutes ago

5 info Committed container10 minutes ago

6 info Committing container10 minutes ago

7 info Packed container10 minutes ago

8 debug Packed file analysis.py (18054 bytes)10 minutes ago

9 debug Packing file analysis.py (18054 bytes)10 minutes ago

10 info Packing container10 minutes ago

11 info Created container10 minutes ago

12 info Creating container10 minutes ago

13 info Built image10 minutes ago

14 info Building image10 minutes ago

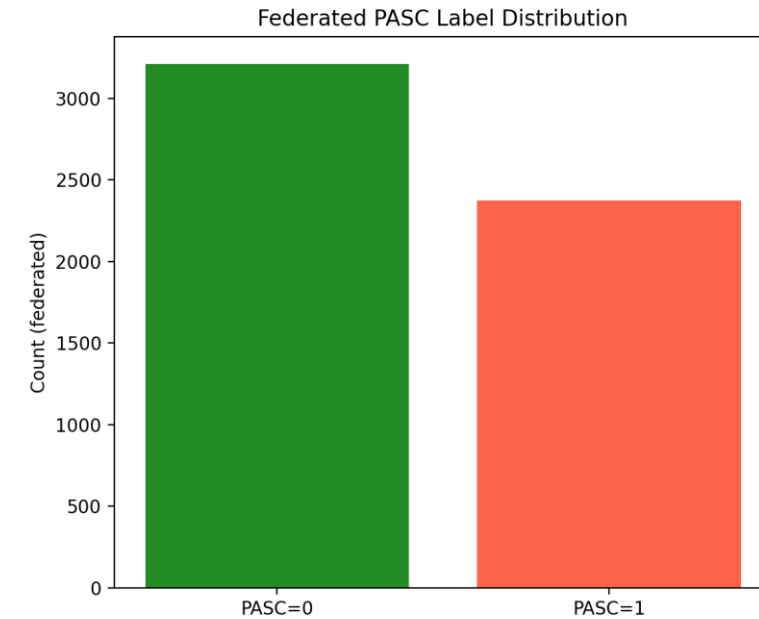
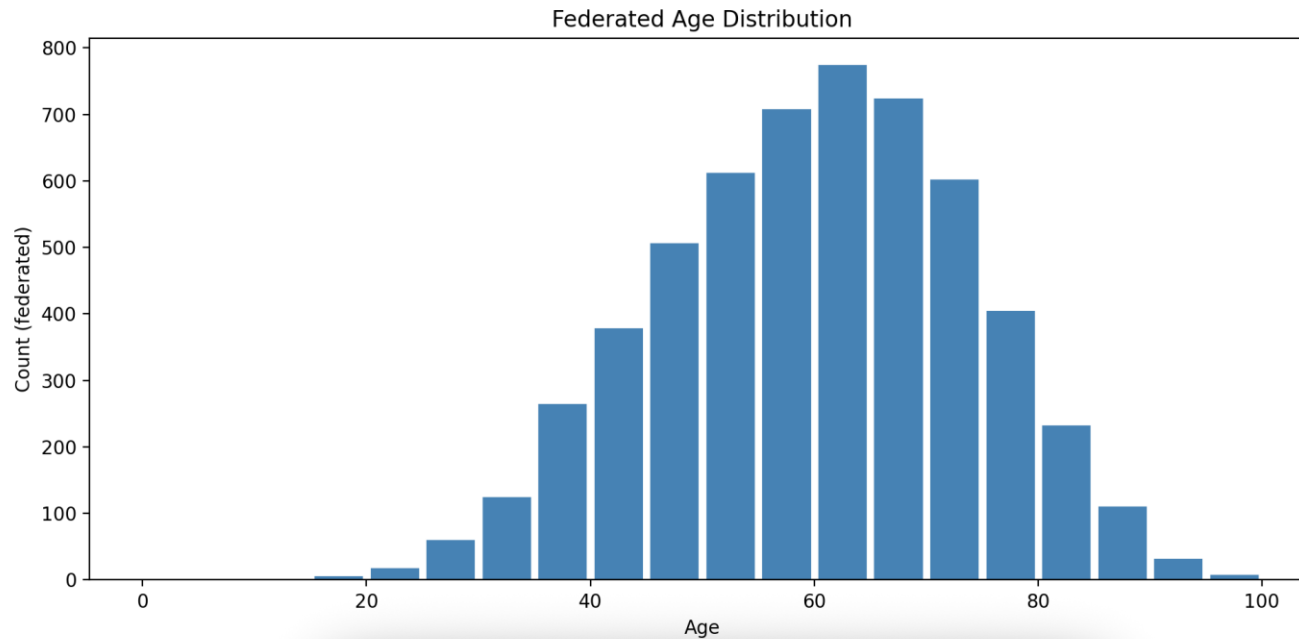
The session will be renewed in 48 minutes(s), 49 seconds(s).

With funding from the:



Federal Ministry
of Research, Technology
and Space

FLAME Demo Results



```
dataset_description_federated.txt
=====
HALTA Long Covid -- Federated Dataset Description
=====
Nodes:                2
Total rows:           5596
Columns:              214
Total missing:        888986

Sex distribution:
M: 3198
F: 2398

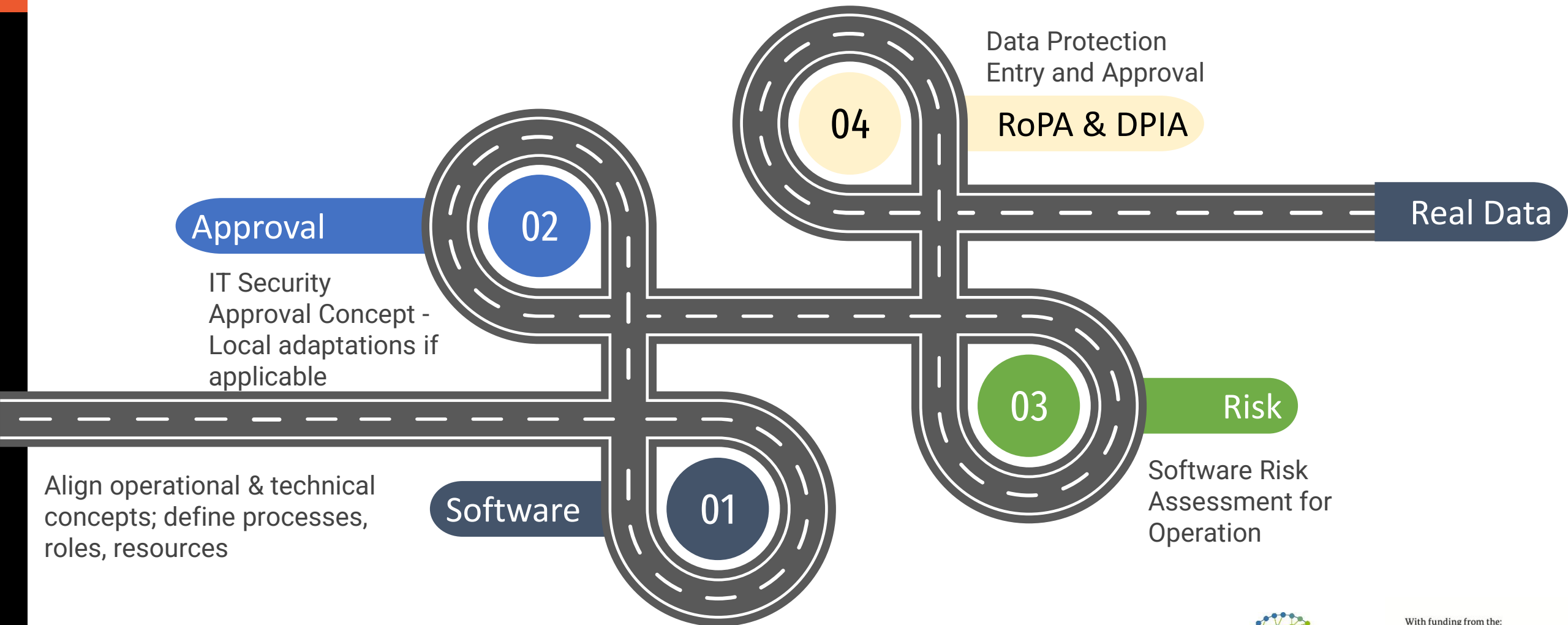
PASC label distribution:
PASC=0: 3217
PASC=1: 2379

Federated SVM accuracy (weighted avg): 0.5182
node bcb3ac02-d73e-43ca-9418-2a7c01b9f58f: acc=0.5254 (n=2798)
node 41bbc50b-a32e-4383-91bb-fbc57b47103b: acc=0.5111 (n=2798)
=====
```

Within a single analysis

- **trained** a Support Vector Machine (SVM)
- performed descriptive **statistical** analyses
- generated **exploratory data visualizations**

Documentation and Deployment Approval



Status and Progress

- Templates for all DP and ITS documentation are available
- Data protection and IT security discussions need to be begun at each site
- Templates are there, but discussion with every site creates new questions
- Platform protections are perceived differently
- Naïve interpretations of data protection (e.g., about data ‘leaving the hospital’) complicate discussions

DIC	Test System	Production System	Docs
Leipzig	ready	ready	ready
Tübingen	ready	ready	ongoing
Berlin	ready	ongoing	ongoing
Erlangen	ongoing	ongoing	ongoing
Munich	ongoing	ongoing	ongoing
Freiburg	ongoing	ongoing	ongoing
Mannheim	ongoing	ongoing	ongoing
Heidelberg	ongoing	ongoing	ongoing
Ulm	ongoing	ongoing	ongoing
Cologne	ongoing	ongoing	ongoing

Next Steps – From Platform to Sustainable Infrastructure

Ongoing

- Onboarding the remaining DICs
- Establishing and simplifying data protection clearing processes
- Getting final production clearance from all DICs
- Interoperability & collaborations (**FLOWER.AI & Vantage6**)

Challenges

- Learning from the projects to simplify processes
- Sustainable funding to keep the platform alive
- Finalize integration with FDPG

Demo Instance Access



Try it hands-on

- Dedicated testing infrastructure
- Synthetic data only — safe to explore
- Full hands-on access to the platform

Request access



Scan the code or email Dr. Marius Herr — he'll share the access details

marius.herr@uni-tuebingen.de

Acknowledgements



Repositories

github.com/PrivateAIM



Info page

privateaim.de



Documentation

docs.privateaim.net



With funding from the:



Federal Ministry
of Research, Technology
and Space