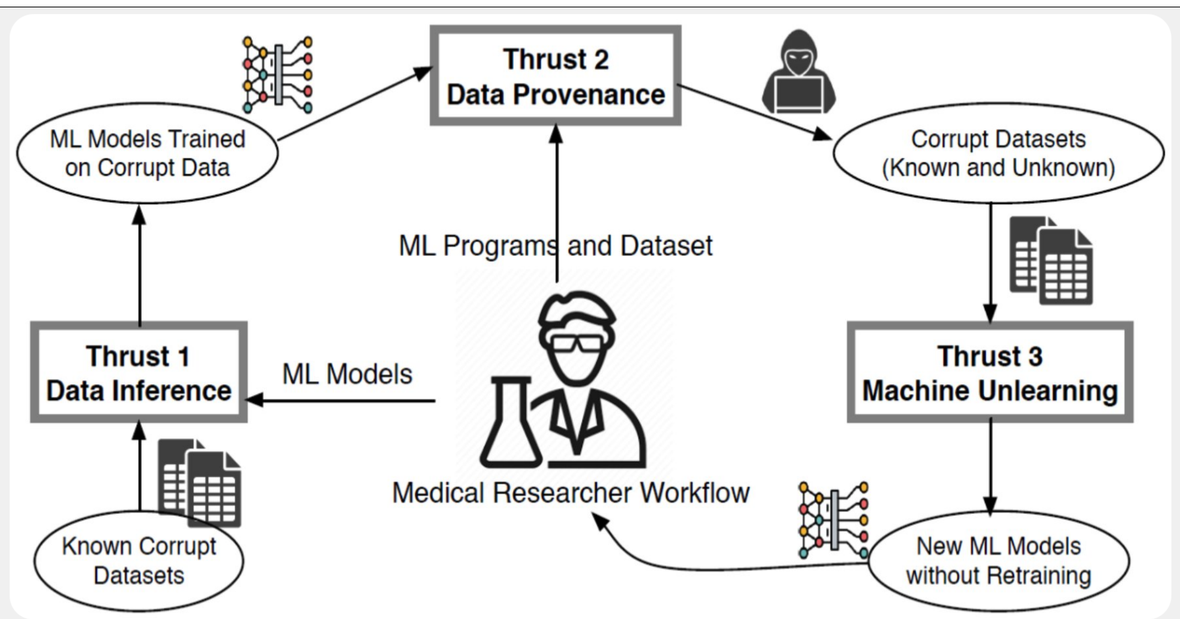
CICI: IPAAI: A Data Provenance Framework for Medical Machine Learning Research # 2531140

Yuan Tian (UCLA), Aichi Chien (UCLA), Yanyan Zhuang (UCCS). Presenter: Zihang Xiang

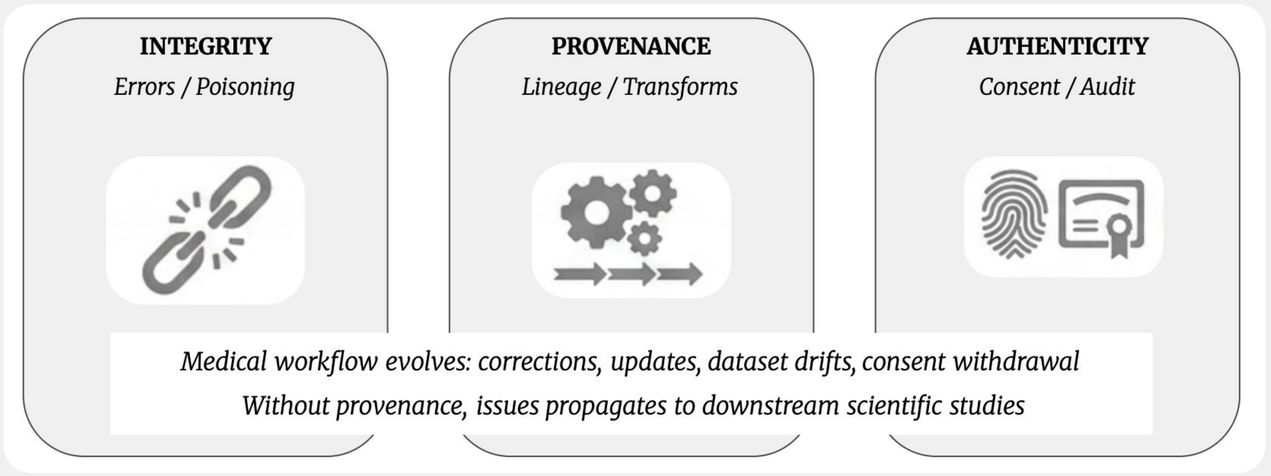
Project Overview

- Infer whether shared models used compromised datasets
- Log dataset lineage / transformations across ML workflows
- Unlearn corrupt data without full retraining
- Store models provenance securely in cyberinfrastructure



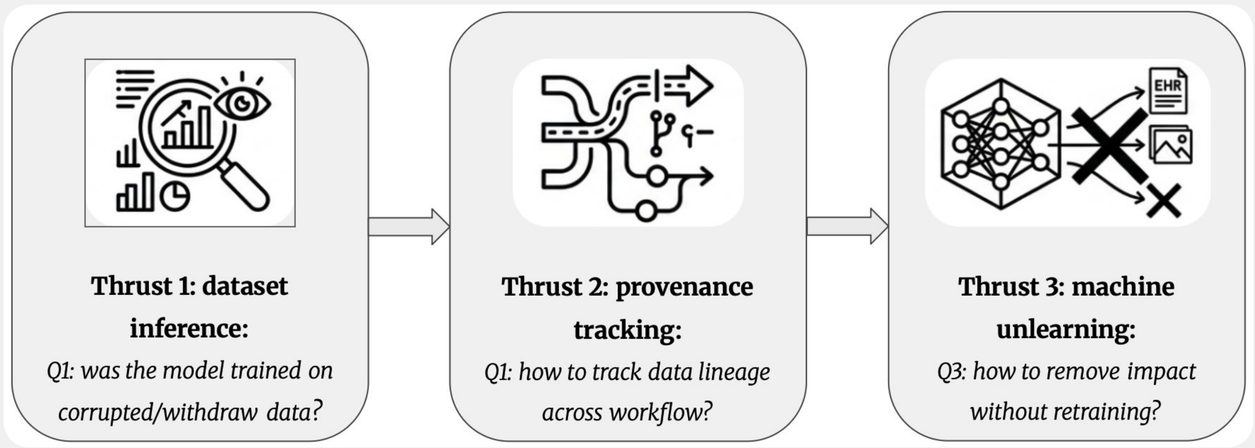
Need for Integrity, Provenance and Authenticity (IPA):

- Detect public ML models trained on corrupt data
- Standardize efficient, reproducible dataset–model tracking
- Remove patient or corrupt data from models effectively

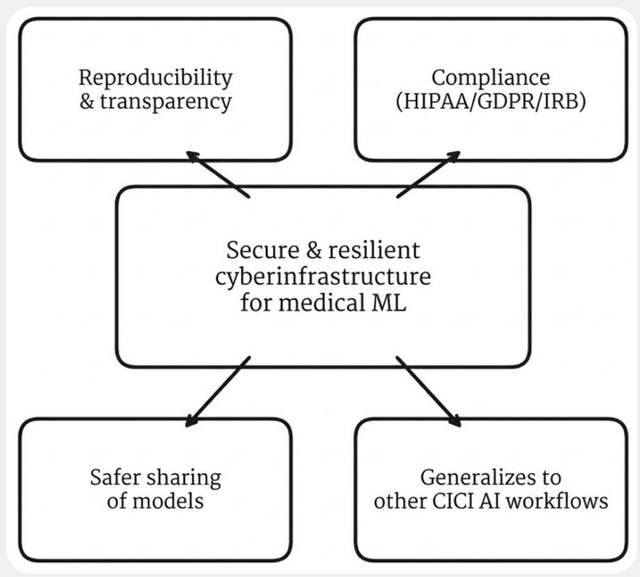


Technical approaches:

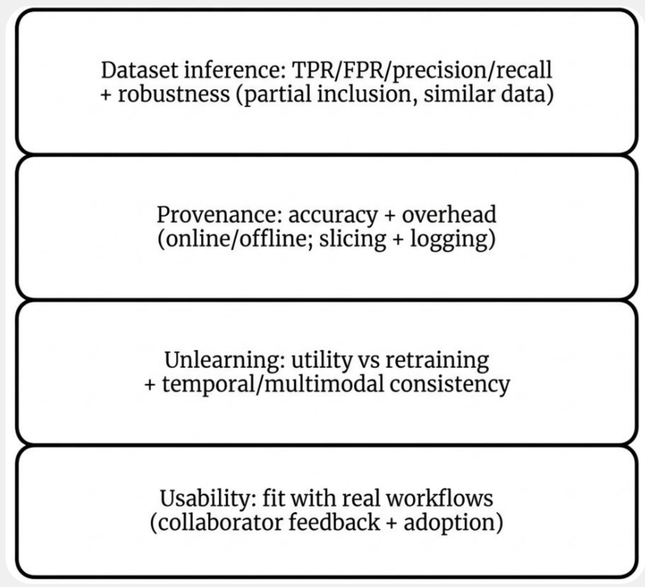
- Thrust 1: dataset inference
- Thrust 2: provenance
- Thrust 3: unlearning



Resulting benefits:



Evaluating and demonstrating IPA:



Risks versus potential for advances: