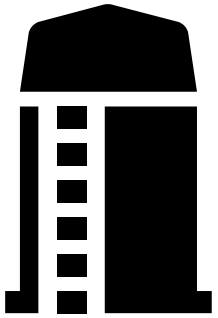
International Tech & Data Conference

Privacy & Pandemics: Responsible Uses of Technology & Health Data

G Anthony Reina, M.D., Chief AI Architect, Health & Life Sciences

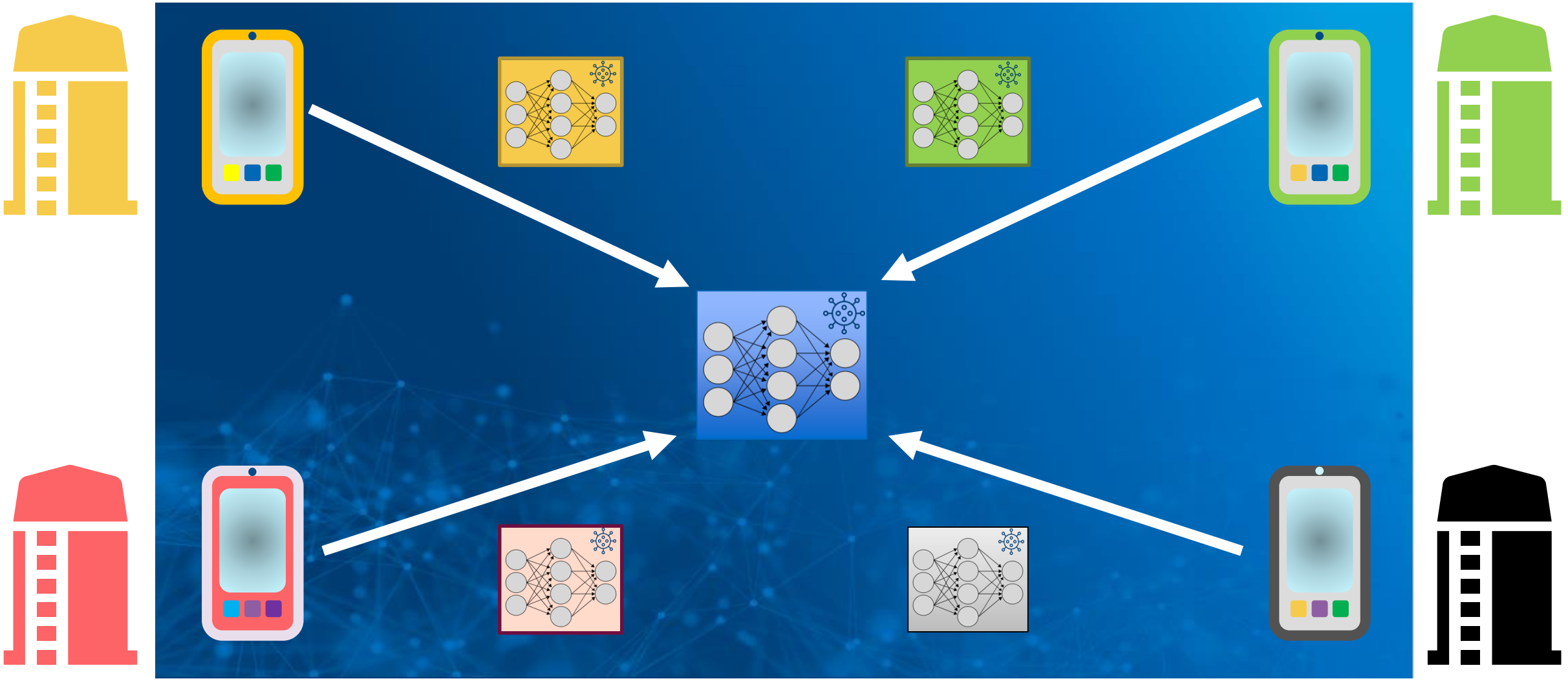
intel®

THE DATA SILO PROBLEM



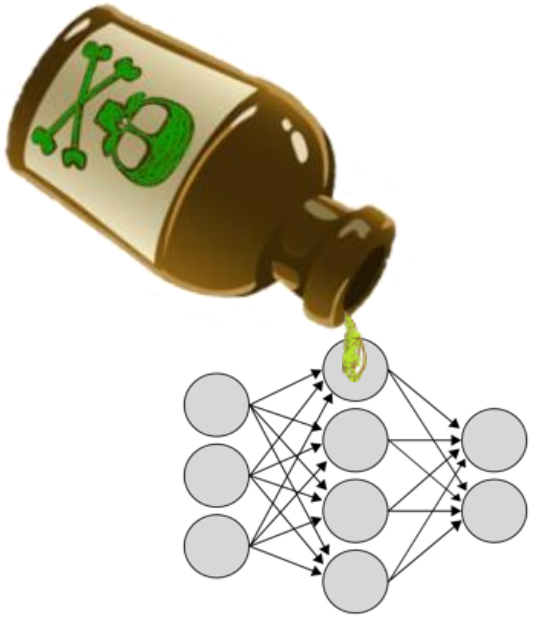
- Privacy / Legality (HIPAA / GDPR)
- Data too valuable (or unknown value)
- Data too large to transmit

FEDERATED LEARNING = NO MORE SILOS

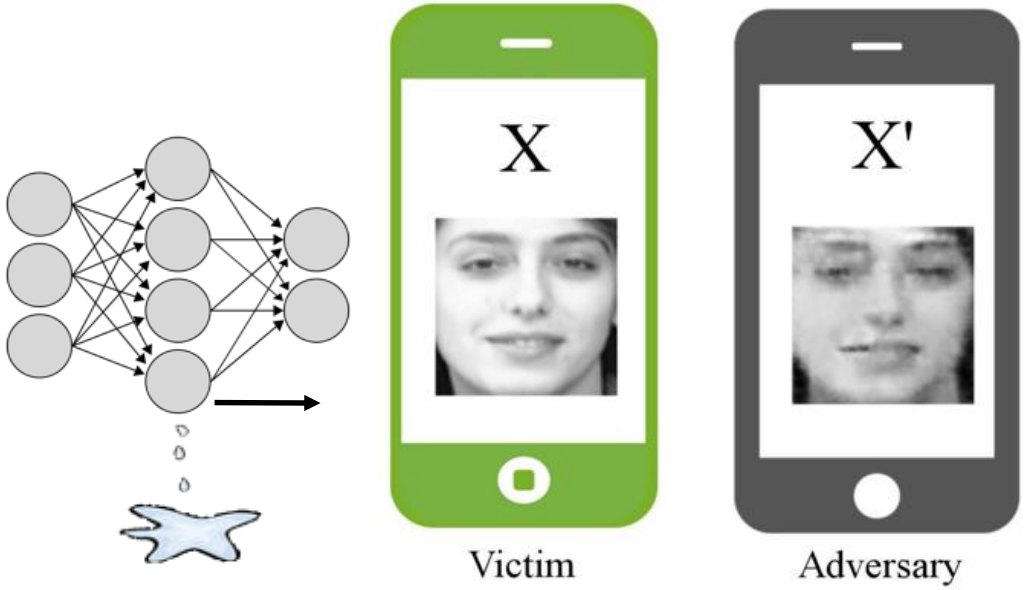


ai.googleblog.com/2017/04/federated-learning-collaborative.html

FEDERATED LEARNING (FL) COULD INCREASE SECURITY AND PRIVACY RISKS



Poisoning attacks may maliciously **alter** models.



Extraction attacks **recover training data** from models.

FL needs to have additional **security** to manage these risks.

Notices and Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.


intel