



# Are You Ready for Production Federated Learning?

Practical readiness considerations for dependable multi-site deployment

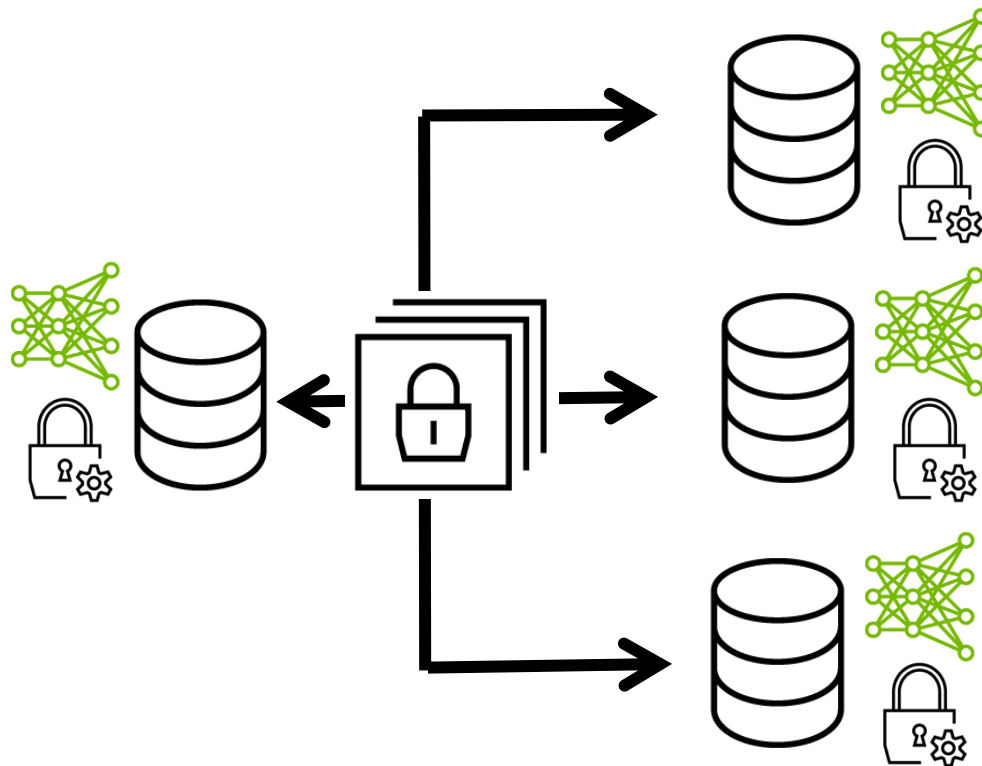
Holger Roth, Chester Chen, Peter Cnudde

NVIDIA

TPC'26 Baltimore, May 2026

# The Decentralized Equation

Data is the key to generalizable AI, but regulations and privacy laws limit access.



## No Raw Data Copy

Central aggregation is impractical.



## Compliance

Strict data sovereignty restrictions.



## Privacy Technologies

Layered controls: encryption, DP, secure aggregation, confidential computing

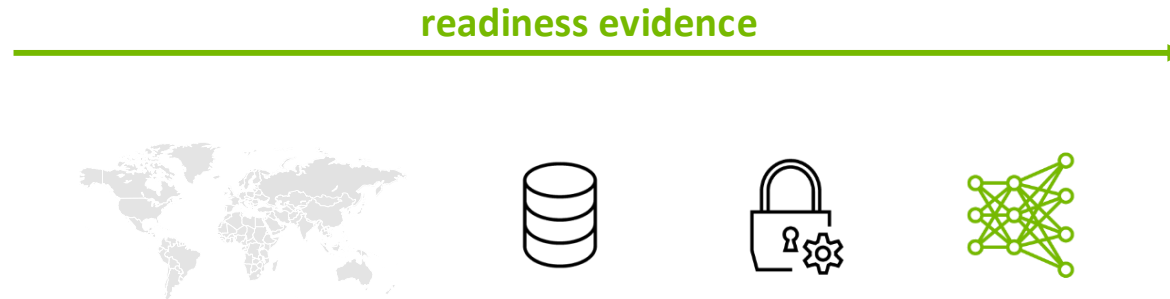


# FL Pilots vs. Production

A trained model is only one artifact in a multi-site deployment.

## Pilot Mindset

- Few sites
- Manual approvals
- Custom scripts
- Best-effort monitoring



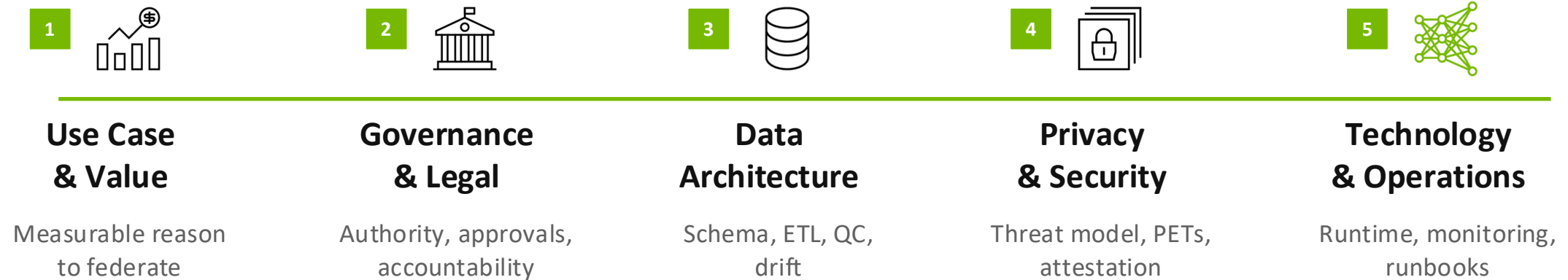
## Production Mindset

- Reusable onboarding
- Evidence-based approvals
- Versioned pipelines
- Observable operations

**Real-world FL fails when value, data, security, or operations are treated as afterthoughts.**

# The 5-Domain FL Readiness Framework

Assess readiness before scaling sites, modalities, workflows, or regulatory exposure.



**The Rule:** Assess each domain with evidence, not opinions.  
Evidence gaps become remediation plans — or a reason not to scale yet.

Evidence gaps tell us exactly what to fix next before scaling.

# Domains 1 & 2: Purpose and Permission

A federation needs a reason to exist — and a durable operating agreement.



## Domain 1: Use Case & Value

- ❖ Narrow, testable clinical/scientific/business questions.
- ❖ Site-level data availability.
- ❖ Pre-agreed success thresholds.



## Domain 2: Governance & Legal

- ❖ Accountable operating model
- ❖ Approval path for the use case
- ❖ Collaboration terms

Production checkpoint

**Why federation, who can decide, and what approvals or terms are needed?**

# Domain 3: Harmonized Inputs, Raw Data Stays Local

Data is only compatible if sites can produce harmonized, validated, versioned inputs.



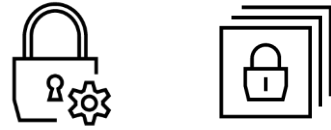
## Minimum evidence

- **Common data model** with versioned ETL.
- **Quality control**: completeness, drift, label quality.
- **Modality compatibility** checks.

Same schema  $\neq$  same meaning

# Domain 4: Privacy & Security in FL

Production FL needs layered controls that map to explicit threats and release risks.



## Defense in depth

- ❖ **Who can connect?** Identity, authorization, certificates, and key management
- ❖ **What can move?** Model updates, metrics, logs, and outputs, protected with appropriate PETs
- ❖ **Where can it run?** Trusted execution and attestation for higher-assurance environments

## Production evidence

### 1 Threat Model

What are the attack scenarios and sensitivities?

### 2 Control rationale

Which PETs and runtime controls are justified?

### 3 Release risk check

Is it safe to share the model, metrics, or outputs?

**Principle:** Use FL to reduce data movement, then use controls to manage residual risk.

# Domain 5: Resilient Technology & Operations

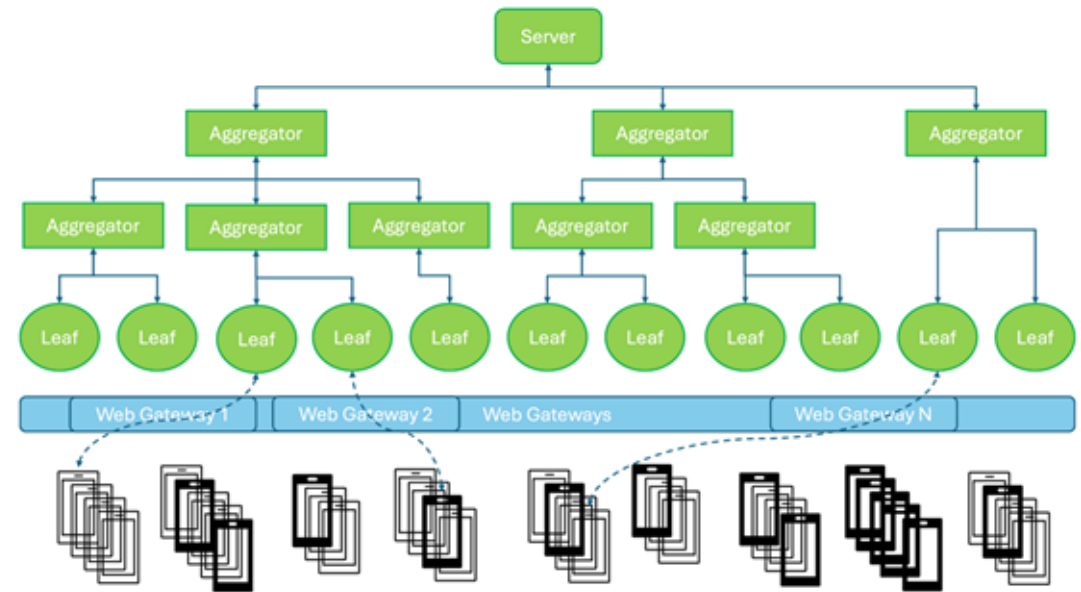
The platform must be reproducible, observable, and resilient across sites.

## Operational capabilities

- ❖ **Connect sites reliably:** Onboarding, networking, access checks
- ❖ **Run consistently across environments:** Approved runtimes from on-prem/device to cloud/HPC
- ❖ **Observe and recover:** Monitoring, incidents, rollback, offboarding

## Reference implementation lens:

**NVIDIA FLARE** provides workflow/runtime hooks for distributed workflows, secure execution, federated evaluation, and monitoring — but readiness still depends on site evidence and process discipline.



Scaling patterns: hierarchical federation, Kubernetes/Slurm, large-model communication

# Make readiness a decision, not a feeling

Minimum evidence turns assumptions into remediation plans and go/no-go signals.

Domain	Production-ready when...
Use Case & Value	The value case, sites, and success criteria are clear
Governance & Legal	Accountable owners and approvals are in place
Data Architecture	Inputs are harmonized, versioned, and quality-checked
Privacy & Security	Controls map to threats and release risks
Technology & Operations	The federation is observable, supportable, and recoverable

Do not ask only “can we train it?” Ask, “can we operate it, audit it, and change it safely?”

# Learn more about FL Use Cases

## NVIDIA FLARE Days

Next event: September 16 & 24, 2026

### US + EMEA Day



Talk

#### Opening Remarks

Ankit Patel, NVIDIA

Opening remarks, NVIDIA Developer Program



Talk

#### What Is NVIDIA FLARE

Holger Roth, NVIDIA

Introduction to NVIDIA FLARE and main features.



Talk

#### The Cancer AI Alliance

Jeff Leek, Fred Hutchinson Cancer ...

The Cancer AI Alliance (CAIA, <https://www.canceralliance.ai/>) is a public-private partnership between...

See All < >

### APAC Day



Talk

#### Keynote: Challenges ...

Han Yu, Nanyang Technological Uni...

The rise of large foundation models underscores the importance and relevance of federated learning as a...

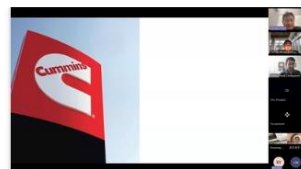


Talk

#### Transforming Cancer...

Shannon McWeeney, OHSU Knight ...

Artificial intelligence (AI) and machine learning (ML) are reshaping oncology, offering powerful tools ...



Talk

#### Federated Learning f...

Vishnu Pandi Chellapandi, Cummin...

Thermal overshoots in diesel aftertreatment systems—particularly at the diesel oxidation ...

See All < >

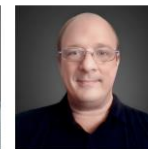
### NVIDIA FLARE Day Speakers



**Jeff Leek**  
Fred Hutchinson Cancer Center, Chief data officer and vice president, and J. Ott Edson Foundation, chair of biostatistics



**Johan Bryssinck**  
Swift, Head of Federated AI AI Team



**Christopher James Langmead**  
Amgen, Scientific Executive Director



**Eric Boenert**  
Rico, Product Manager for Federated Open Science



**Han Yu**  
Nanyang Technological University (NTU), Associate Professor



**Yuval Baror**  
Rhino FCR, Cofounder and CTO



**Robin Rohm**  
Apheris, CEO & Cofounder



**Adi Hirschstein**  
Quality Technologies, Vice President of Product



**Prof. Dr. Chien-Chang Lee, MD, PhD**  
Ministry of Health and Welfare (MOHW), Taiwan, Chief Information Officer and National Taiwan University Professor, Staff Physician



**Gregg Spivey**  
Eli Lilly & Company, Senior Director, AI/ML Business Strategy Lead

### See All Speakers



**Chester Chen**  
NVIDIA, Senior Product and Engineering Manager, FLARE



**Ankit Patel**  
NVIDIA, Senior Director Developer Marketing



**Yan Cheng**  
NVIDIA, Director of Software Engineering, FLARE Chief Architect



**Rahul Choudhury**  
NVIDIA, Senior Software Engineering Manager, Holoscan



**Ziyue Xu**  
NVIDIA, Senior Data Scientist



**Adrish Sannysasi**  
Rhino FCR, Vice President of Customer Solutions



**Holger Roth**  
NVIDIA, Principal Federated Learning Data Scientist



**Duy Phuong Nguyen**  
Iowa State University, Ph.D. student



**Johnny Wang**  
Toyota, Principal Researcher



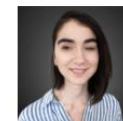
**Nikolas Koutsoubis**  
USF/Moffitt Cancer Center, Ph.D. Student



**Sara Okhuijsen**  
GASYS NOW, CTO



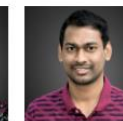
**Christoph Angerer**  
NVIDIA, Senior Manager, HPC Developer Technology Group



**Zühal Tannur**  
Neurovision AI Tech, Founder and CEO



**Shannon McWeeney**  
OHSU Knight Cancer Institute, Professor and Chief Data Officer



**Vishnu Pandi Chellapandi**  
Cummins Research and Technology, Senior Technical Specialist



**Max Carlson**  
Sandia National Labs, Postdoc data scientist



**Chris Siefert**  
Sandia National Labs, Research Scientist



**Gaurav Tripathi**  
Innoplexus (Partec), Group CTO



**Po-Chun Liao, MSc**  
Ministry of Health and Welfare (MOHW), Taiwan, Chief Engineer, Industrial Technology Research Institute (ITRI) and Chief Engineer for Federated Learning



Past recordings: [developer.nvidia.com/flare-day-2025](https://developer.nvidia.com/flare-day-2025)



**Thank you!**

**Discussion:** What should we standardize first so that federated learning can move more reliably from pilots to production?

**Contact:** Holger Roth <[hroth@nvidia.com](mailto:hroth@nvidia.com)>

**Try out NVIDIA FLARE!**

[github.com/NVIDIA/NVFlare](https://github.com/NVIDIA/NVFlare)