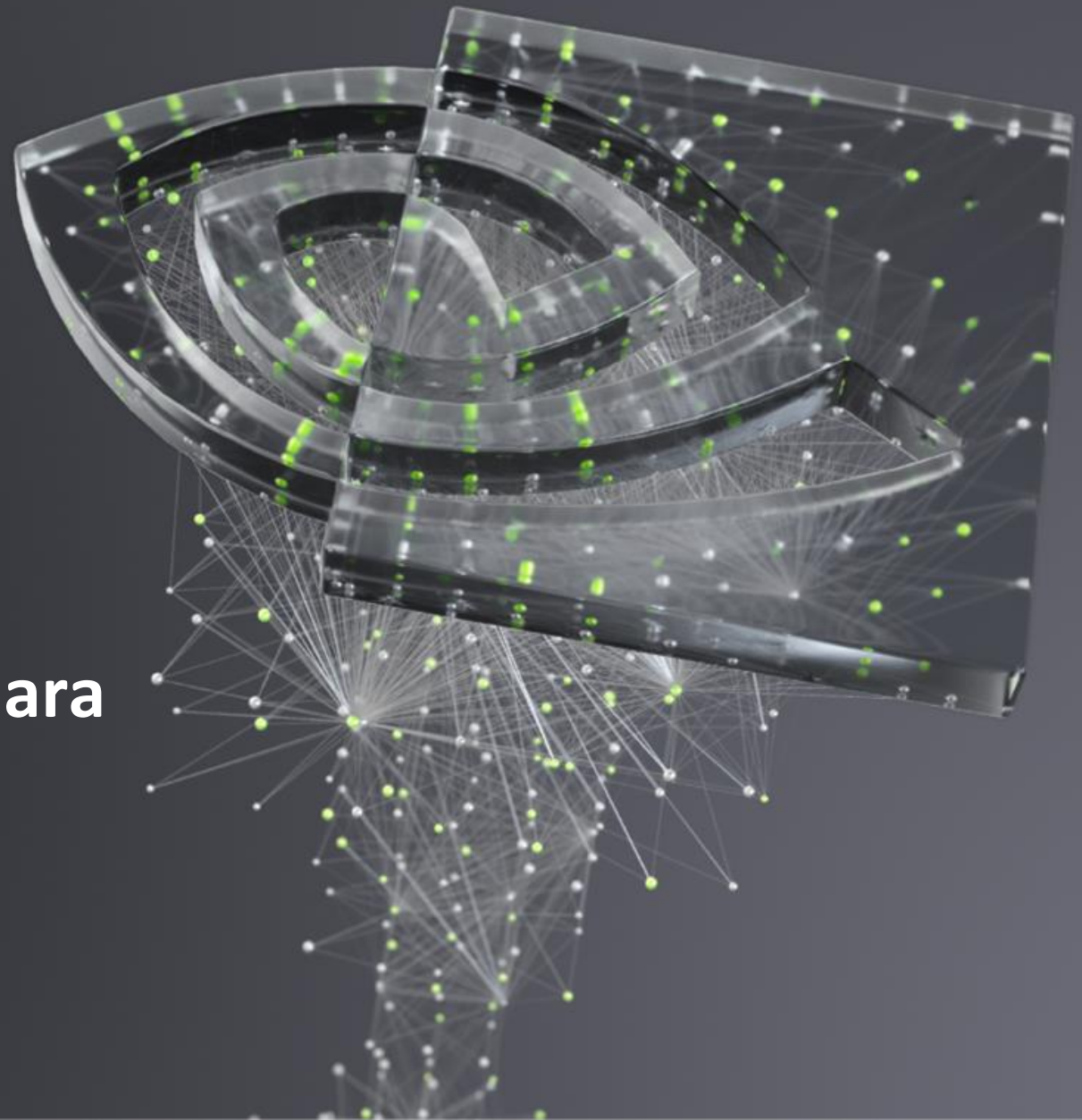


Federated Learning with Clara

Warren Tseng
Solution Architect
Healthcare, Taiwan

CLARA FEDERATED LEARNING

Collaborative Distributed Learning

Addressing Data Diversity & Privacy

Distributed Collaborative Learning

Build a common, robust AI model without sharing data

Using NVIDIA Clara to:

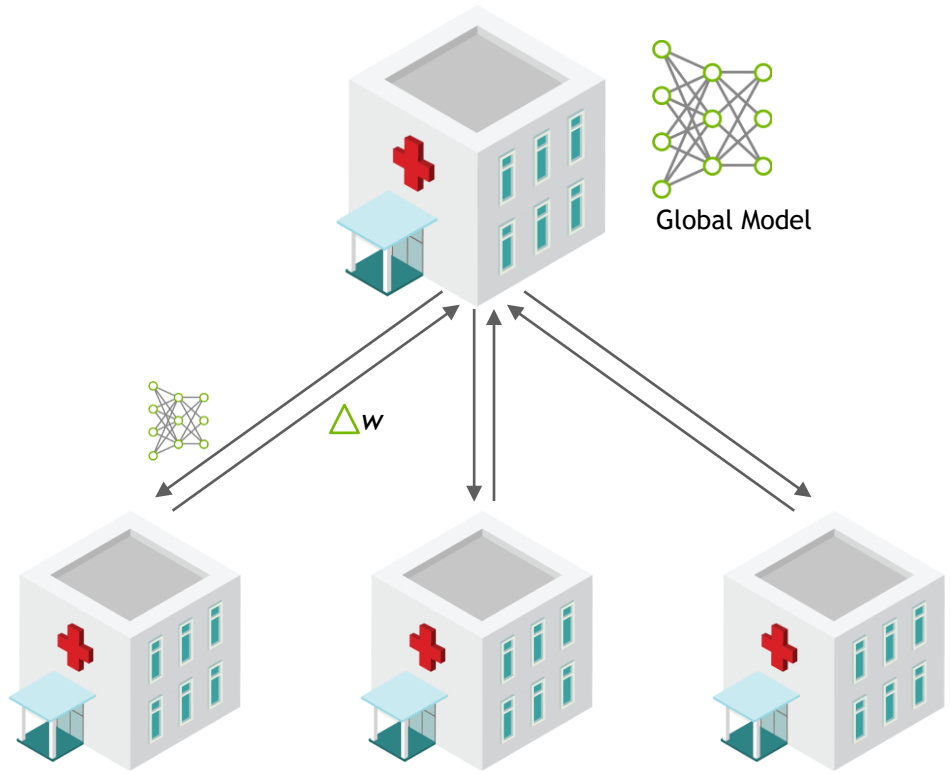
Authenticate and deliver Clara FL to participating hospitals

Locally train on private data

Securely Share partial-model weights

Apply Federated Averaging creating a new global model

BYOC to Federated Learning - New



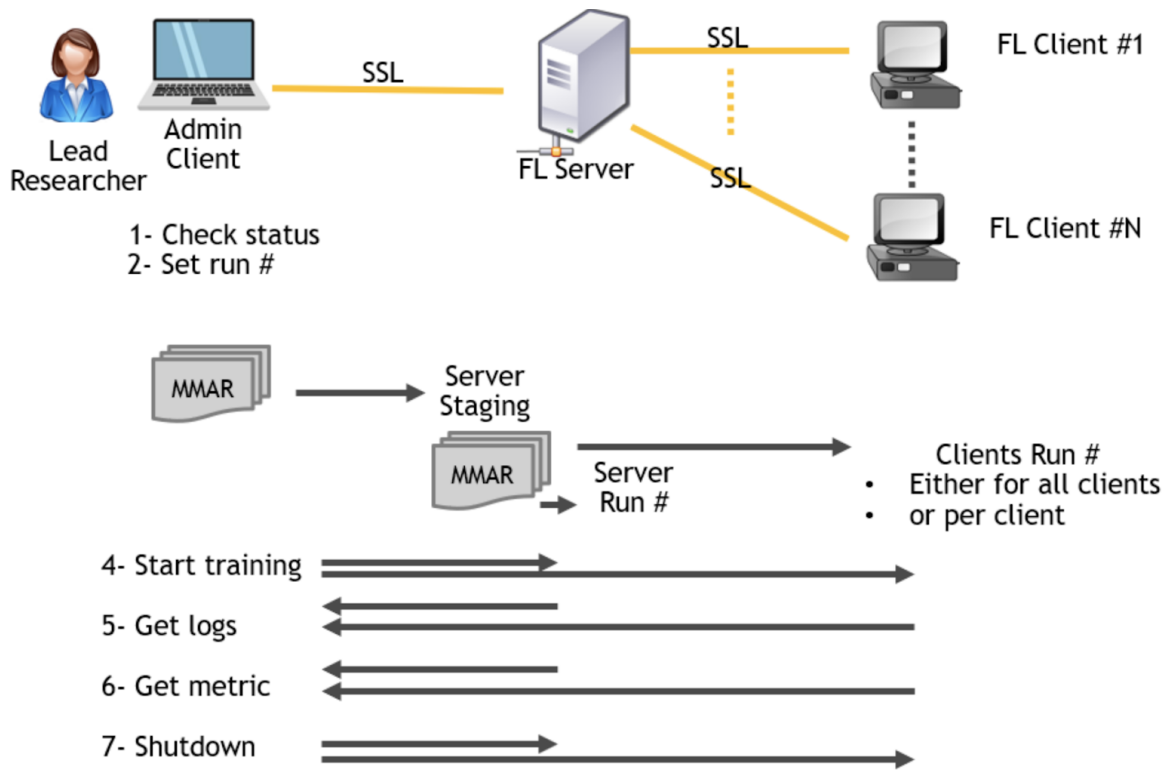
CLARA FEDERATED LEARNING

Collaborative Distributed Learning

Enable easy server and client deployment through the use of an administration client.

Reduce the amount of human coordination involved to set up a federated learning project.

Provide an admin the ability to deploy the server and client configurations, start the server / clients, abort the training, restart the training, and more.



PRIVACY-PRESERVING FEDERATED LEARNING

Reference Differential Privacy Algorithm

Protects Against Model Inversion

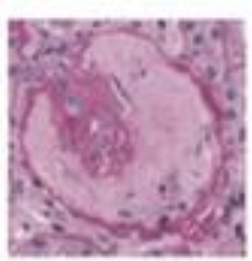
Protect Data Exposed to Model Inversion Attacks

Implicit Training Data Leakage

Privacy Protection Federated Learning

No data sharing amongst contributing sites

Authentication, Authorization & Secure Connection



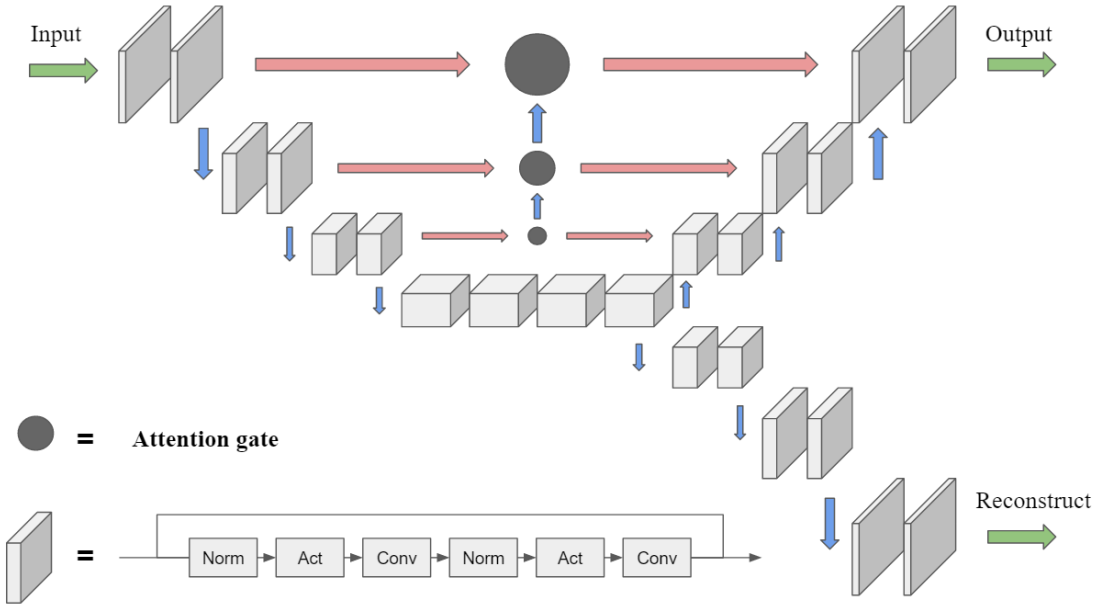
Training image

Model inversion

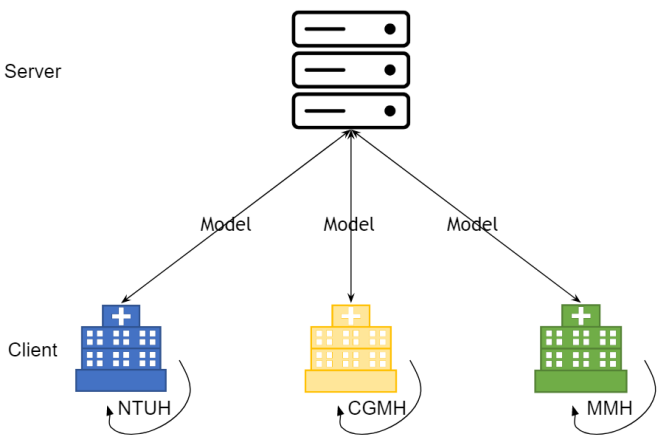
Training image

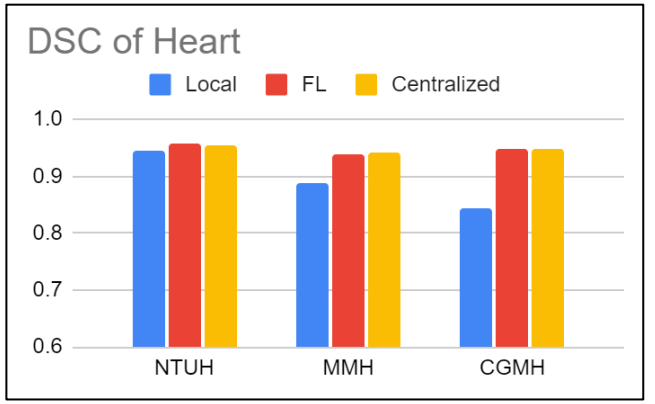
Model inversion

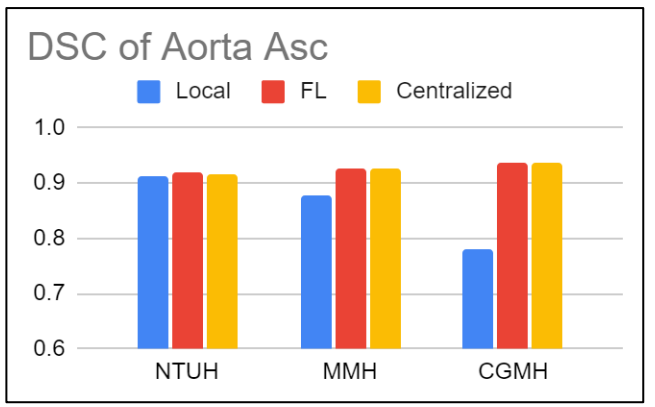
Fredrikson et al. "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures" CCS 2015
Wu et al., "P3SGD: Patient Privacy Preserving SGD for Regularizing Deep CNNs in Pathological Image Classification" CVPR 2019

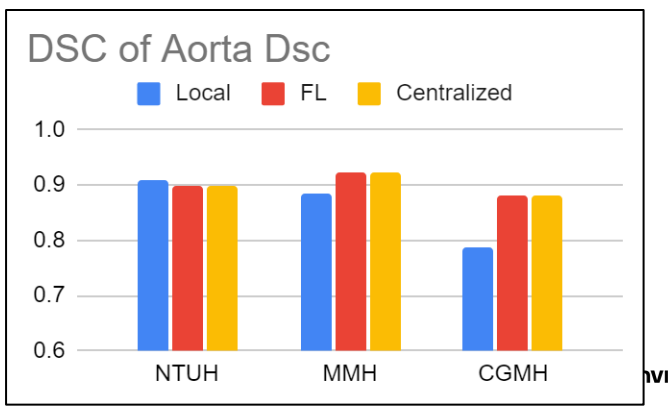


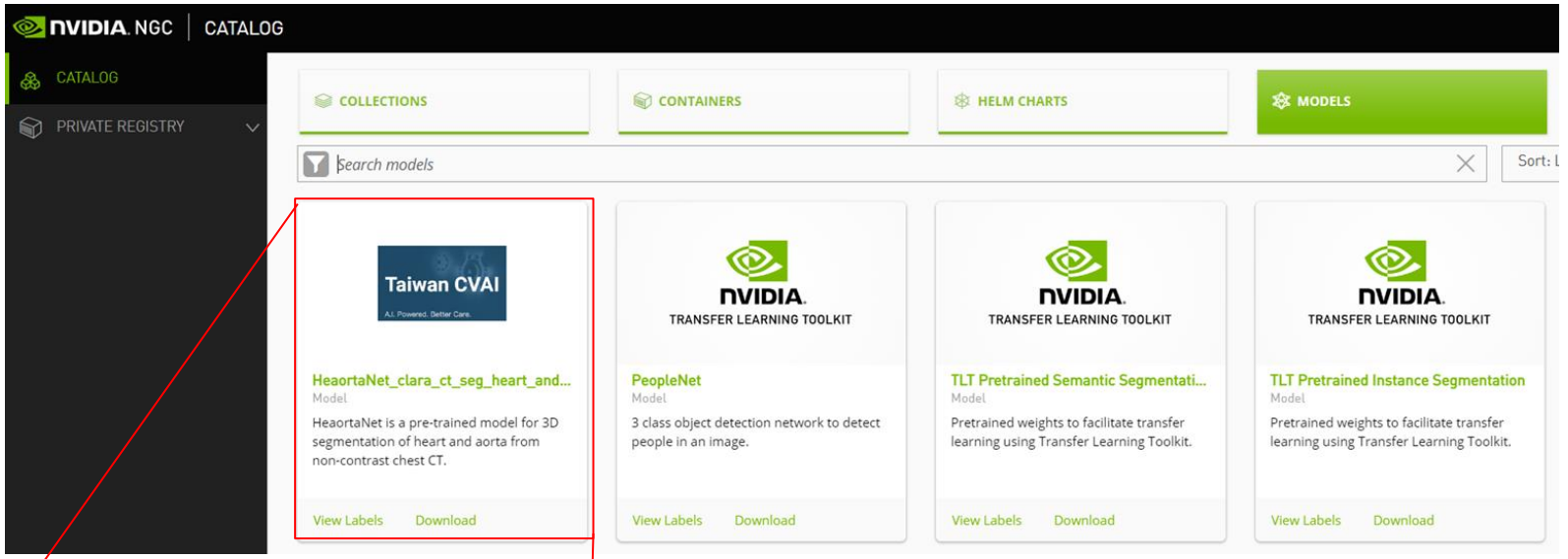
本研究聯合台大、長庚以及馬偕3家醫院之資料，以自行設計之HeaortaNet進行聯邦學習，於大部份指標都有顯著提升。
惟台大醫院降主動脈囊括範圍太廣，與其它醫院資料差異太大，其效果因模型泛化的緣故稍有下降。

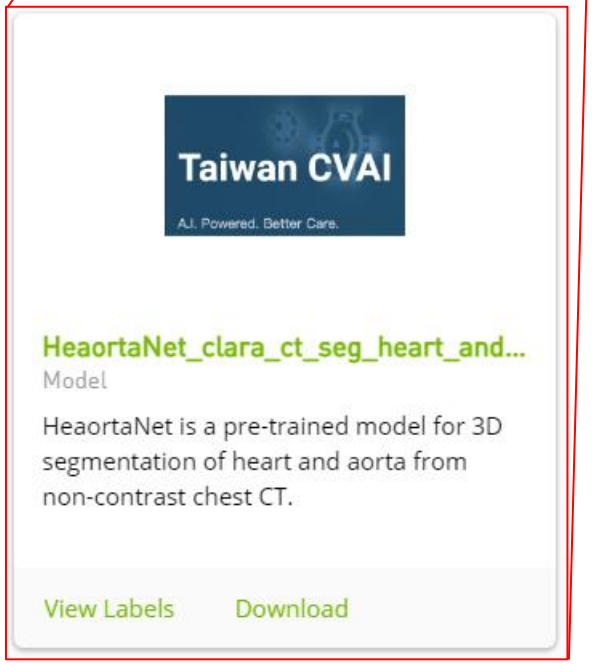


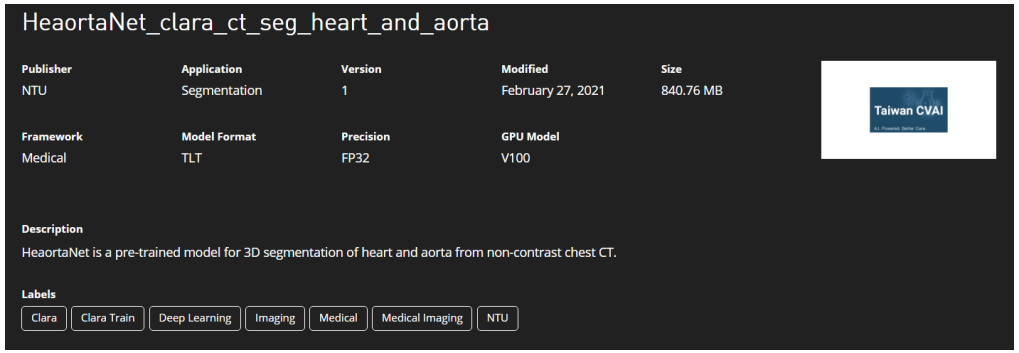












https://ngc.nvidia.com/catalog/models/nvidia:med:heaortanet

本研究團隊與NVIDIA Taiwan合作開發之HeaortaNet率先取得NVIDIA HQ認證，為全球第一個發佈於NVIDIA GPU Cloud (NGC) 平台的合作夥伴開發模型，供全球開發者互相交流使用

NVIDIA

Taiwan CVAI
A.I. Powered. Better Care.

MeDA

CATALOG

PRIVATE REGISTRY

BATCH

Catalog: Models / **Models: nvidia:med:clara_xray_classification_chest_no_amp**

clara_xray_classification_chest_no_amp

Publisher	Application	Version	Modified	Size
NVIDIA	Classification	1	September ...	417.68 MB

Framework	Model Format	Precision	GPU Model
Medical	TLT	FP32	V100

Description

clara_xray_classification_chest_no_amp is a pre-trained densenet121 model for disease pattern detection in chest x-rays.

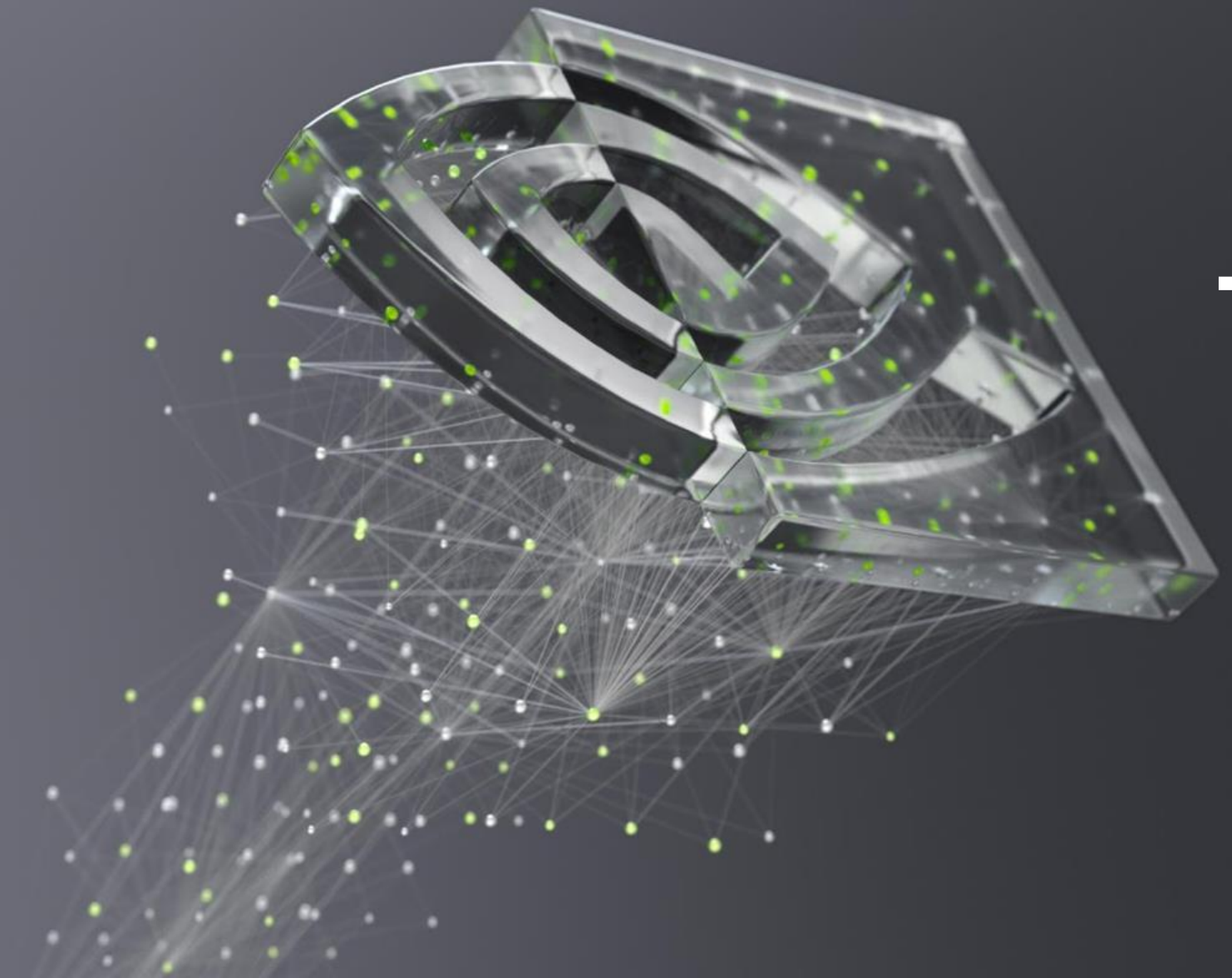
Labels

Deep Learning | Medical Imaging

Wget Model | CLI Command

```
$ wget --content-disposition
https://api.ngc.nvidia.com/v2/models/nvidia/med/clara_xray_classification_chest_no_amp/versions/1/zip -O clara_xray_classification_chest_no_amp_1.zip
```

Overview | Version History | File Browser | Related Collections



Thank you

Warren Tseng
wtseng@nvidia.com

NVIDIA