

Vivli AI/ML Model Requirements

The AI/ML requirements were developed to ensure responsible practices and compliance with our data governance and export policies. We have established a set of baseline requirements that all AI/ML models must meet prior to entering the review and approval process. These criteria apply to all externally developed or submitted models.

1. AI/ML models permissible to be imported to the Vivli Environment

All models must adhere to the following standards:

- A. Models **must be untrained** on external data or be trained on **anonymized** data. (i.e. Anonymized data is contained in the model - Model is trained on and includes anonymized data. Anonymized data results from removing personal identifiers, aggregating data, or processing this data in a way that it can no longer be related to an identified or identifiable individual. (Example: clinical trial/registry data that is anonymized))
- B. Models that are trained on de-identified or identifiable data are not allowable. (For example, de-identified data is contained in the model - Model is trained on and includes de-identified data. De-identified or pseudonymized data results from the processing of personal data such that the personal data can no longer be attributed to a specific data subject without the use of additional information. These terms are distinguished from anonymization, as the code exists to link the data back to the individual. (Example: clinical trial data that has identifiers de-identified, pseudonymized))

2. AI/ML models permissible to be exported from the Vivli Environment

Only traditional **machine learning** models are approved for export and integration:

- **Permitted model types** include for example:
 - Lasso Regression
 - Random Forests
 - Support Vector Regression (SVR)
 - Decision Trees
 - k-Nearest Neighbors (KNN)
 - Gradient Boosting
 - Kernel Machines
 - Boosting Algorithms
 - Gaussian Mixture Models (GMMs)
- **Prohibited model types** include for example:
 - Deep learning models (e.g., CNNs, RNNs, Transformers)
 - Generative AI models (e.g., GANs, LLMs)
 - Any model using proprietary, de-identified, or identifiable external datasets

Models falling outside the list of permitted exports or not complying with data import requirements will not proceed to the next stage of the data request review process.