EscrowAI® Product Interface

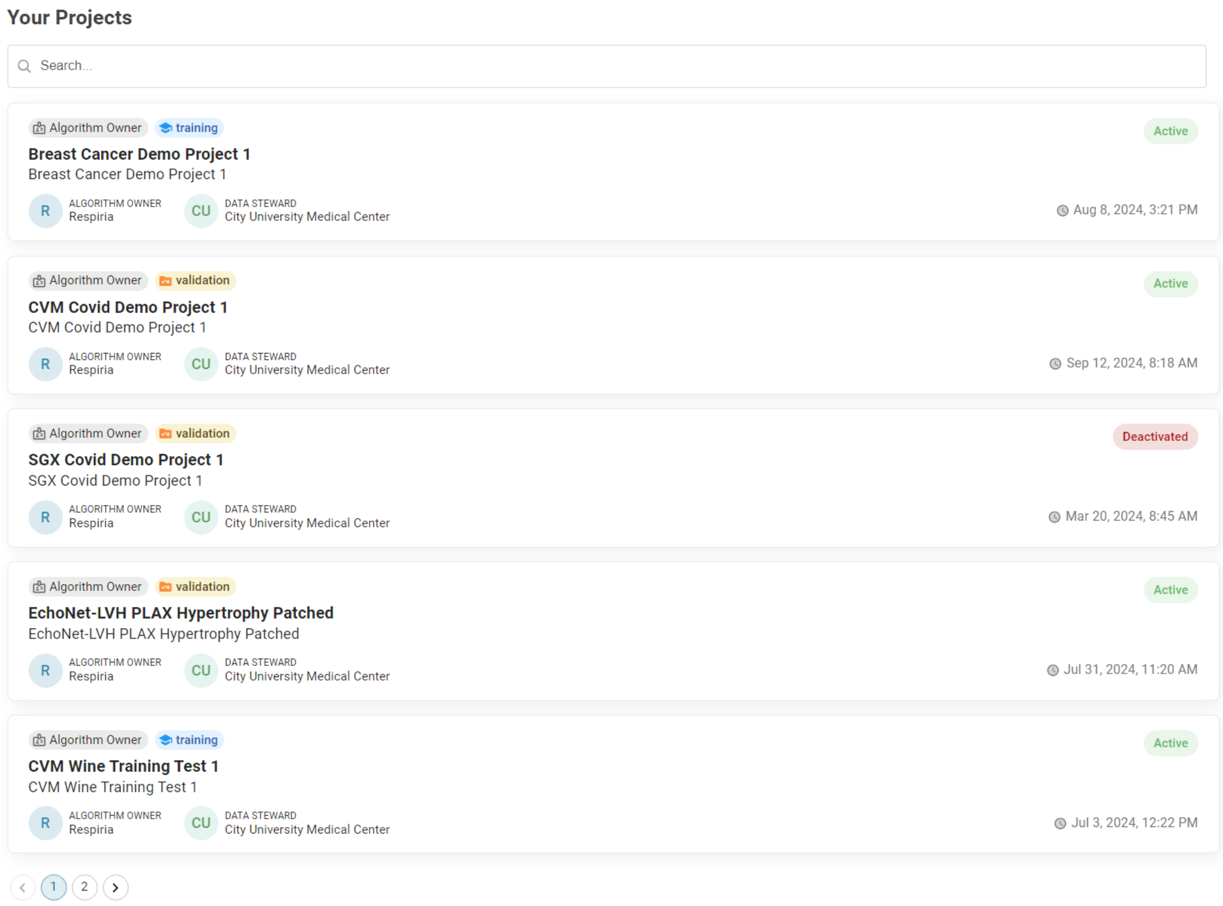
How EscrowAI works

1. An algorithm owner uploads their encrypted algorithm to EscrowAI, specifying either training or validation mode. EscrowAI builds the algorithm into a secure computing container.
2. A data controller curates a data set to meet the algorithm owner's requirements. The data set is encrypted and uploaded to an EscrowAI accessible zone within **their** secure cloud. A secure pointer to that data set is entered into EscrowAI. No data is ever sent EscrowAI, and the data sets are not accessible from outside the data controller's environment.
3. The algorithm owner creates a run configuration for a unique combination of the algorithm and dataset versions.
4. The algorithm owner sends a run request to the data controller.
5. The data steward either initiates the run or rejects it.
6. To run the algorithm, EscrowAI initiates an attested, hardware-based Trusted Execution Environment (TEE) in the Data Steward cloud and loads the secure algorithm container and encrypted data into the TEE. In the attested enclave:
   - The algorithm and data are decrypted in protected memory.
   - The algorithm runs.
   - Standardized training output parameters are sent to the tracking server in a training run and displayed in the reporting interface. The trained model is also available.
   - In a validation run, a confidential report is created containing the algorithm's performance.
   - The run outputs are the only things that leave that secure computing enclave.
7. The TEE is decommissioned.

Projects are coordinated through the EscrowAI interface, a SaaS application. Collaborating parties are brought together in a project framework, and the necessary project artifacts and interactions are managed within EscrowAI. An artifact card structure is used to upload and manage the project inputs and outputs, and a project tracking overview displays the project's progress. EscrowAI uses role-based access control; within a project users interact only with the artifacts they control or to which they require access.

User Landing Page

Users within organizations are assigned to projects, which are listed on their landing page after accessing EscrowAI. Project cards identify the user's role, their collaborating organization, the type of project, and the project's status.



Your Projects

Algorithm Owner · training · Active
Breast Cancer Demo Project 1
Breast Cancer Demo Project 1
R ALGORITHM OWNER Respiria · CU DATA STEWARD City University Medical Center · Aug 8, 2024, 3:21 PM

Algorithm Owner · validation · Active
CVM Covid Demo Project 1
CVM Covid Demo Project 1
R ALGORITHM OWNER Respiria · CU DATA STEWARD City University Medical Center · Sep 12, 2024, 8:18 AM

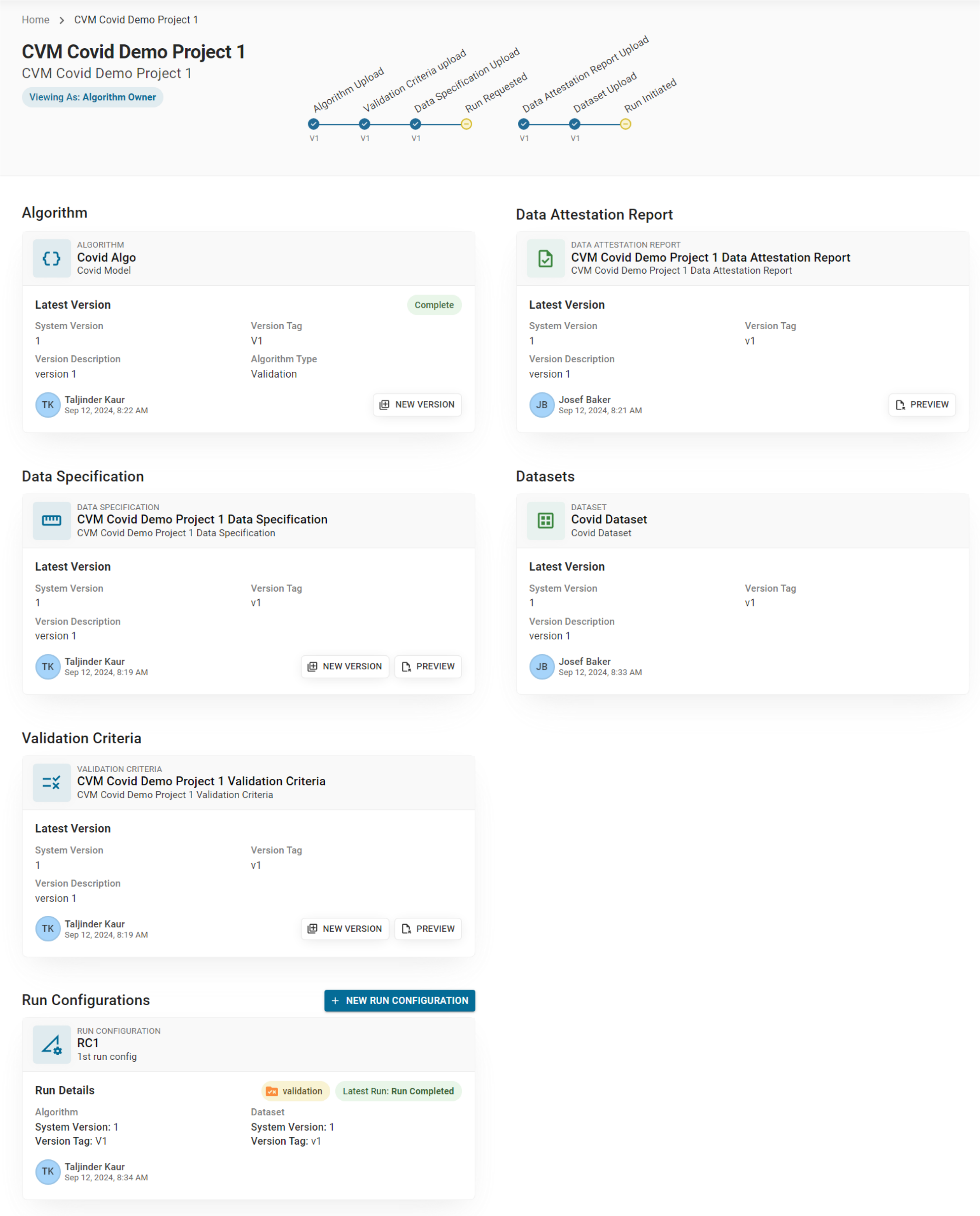
Algorithm Owner · validation · Deactivated
SGX Covid Demo Project 1
SGX Covid Demo Project 1
R ALGORITHM OWNER Respiria · CU DATA STEWARD City University Medical Center · Mar 20, 2024, 8:45 AM

Algorithm Owner · validation · Active
EchoNet-LVH PLAX Hypertrophy Patched
EchoNet-LVH PLAX Hypertrophy Patched
R ALGORITHM OWNER Respiria · CU DATA STEWARD City University Medical Center · Jul 31, 2024, 11:20 AM

Algorithm Owner · training · Active
CVM Wine Training Test 1
CVM Wine Training Test 1
R ALGORITHM OWNER Respiria · CU DATA STEWARD City University Medical Center · Jul 3, 2024, 12:22 PM

Project Interface

The project page is the interactive interface for the collaborators. Each artifact card is the entry point for the activities needed to fulfill the scope of that artifact. For example, entering the Algorithm card exposes the interface for encrypting and uploading an algorithm, adding any meta data associated with the version, and assigning its relationship to the other project artifacts (e.g., an associated data set).



CVM Covid Demo Project 1

CVM Covid Demo Project 1

Algorithm

ALGORITHM
Covid Algo
Covid Model

Latest Version — Complete

System Version 1	Version Tag V1
Version Description version 1	Algorithm Type Validation

TK Taljinder Kaur
Sep 12, 2024, 8:22 AM

Data Attestation Report

DATA ATTESTATION REPORT
CVM Covid Demo Project 1 Data Attestation Report
CVM Covid Demo Project 1 Data Attestation Report

Latest Version

System Version 1	Version Tag v1
Version Description version 1	

JB Josef Baker
Sep 12, 2024, 8:21 AM

Data Specification

DATA SPECIFICATION
CVM Covid Demo Project 1 Data Specification
CVM Covid Demo Project 1 Data Specification

Latest Version

System Version 1	Version Tag v1
Version Description version 1	

TK Taljinder Kaur
Sep 12, 2024, 8:19 AM

Datasets

DATASET
Covid Dataset
Covid Dataset

Latest Version

System Version 1	Version Tag v1
Version Description version 1	

JB Josef Baker
Sep 12, 2024, 8:33 AM

Validation Criteria

VALIDATION CRITERIA
CVM Covid Demo Project 1 Validation Criteria
CVM Covid Demo Project 1 Validation Criteria

Latest Version

System Version 1	Version Tag v1
Version Description version 1	

TK Taljinder Kaur
Sep 12, 2024, 8:19 AM

Run Configurations

RUN CONFIGURATION
RC1
1st run config

Run Details — validation — Latest Run: **Run Completed**

Algorithm System Version: 1 Version Tag: V1	Dataset System Version: 1 Version Tag: v1

TK Taljinder Kaur
Sep 12, 2024, 8:34 AM