

# Deep-Rad: Privacy-Preserving Medical Diagnostics

## Overview

The healthcare industry generates invaluable patient data for diagnostic AI, but its use is restricted by privacy regulations like HIPAA and GDPR. Deep-Rad is a platform that solves this problem using **Federated Learning**, a distributed machine learning approach where the AI model is sent to the data, not the other way around.

## Solution and Implementation

Instead of collecting patient data, our platform sends the AI diagnostic model directly to the data source. Hospitals train the model on their secure, local servers and then send only the model's 'learnings' or weight updates back to a central aggregator. This process is repeated across a network of hospitals to build a robust global model. The implementation includes a secure federated learning platform, specialized medical imaging models, a client-side application for hospitals, and a central model aggregation service.

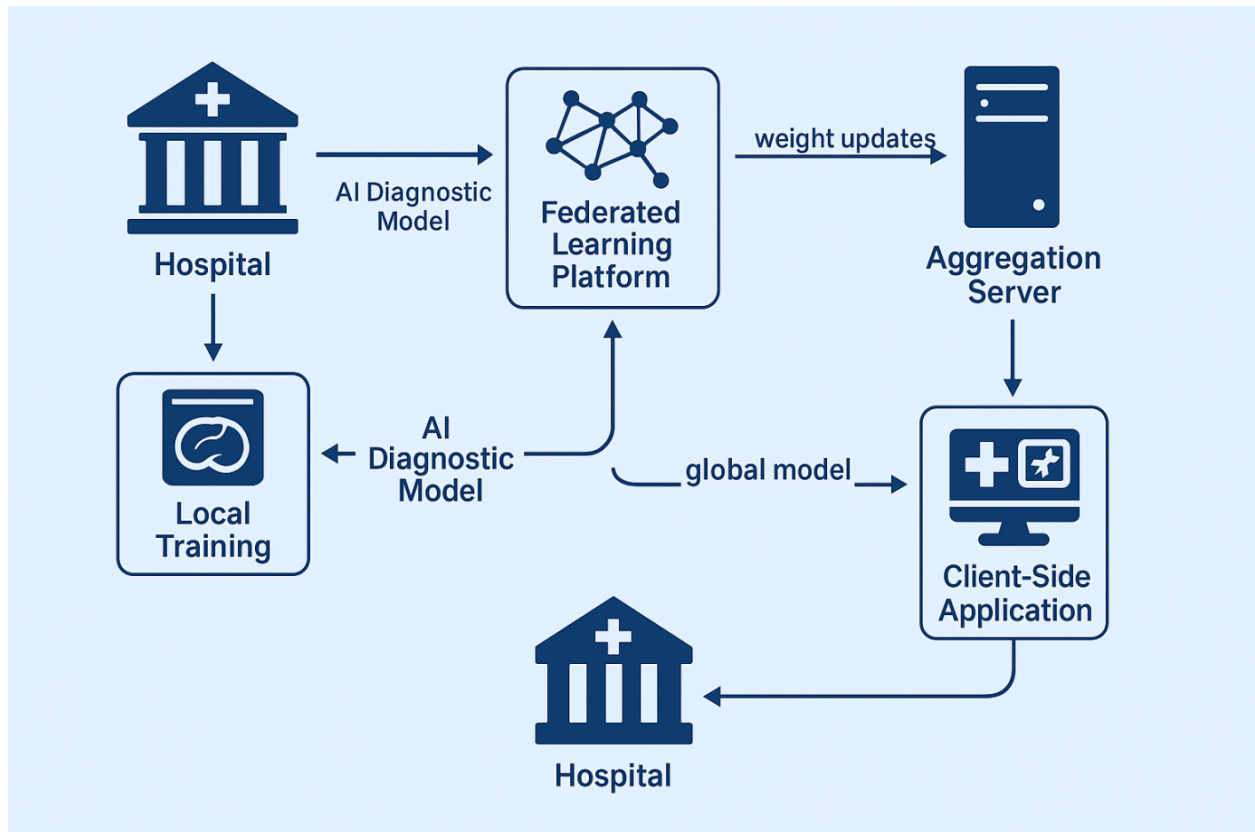
## Objective

The main objective is to enable the development of powerful medical AI without compromising patient privacy. We aim to overcome the legal and logistical barriers associated with centralizing sensitive healthcare data by leveraging the collective intelligence of a network of hospitals.

## Methodology

Our methodology centers on a distributed training framework. A lightweight AI model is distributed to a network of client-side components at various hospitals. Each client trains the model locally and then sends encrypted weight updates back to a central server. The server aggregates these updates, refines the global model, and then securely sends the new model back to the clients. This ensures data remains at its source.

## Highlevel system Diagram:



## Significance

The AI in medical diagnostics market is projected to reach **\$17.1 billion by 2035**. Our federated learning approach is critical for unlocking this market by providing a solution that adheres to the strictest privacy standards. Over **90%** of healthcare institutions are hesitant to centralize sensitive data, representing a vast, untapped market we can access.

## Expected Outcomes

We expect to deliver a secure federated learning platform and specialized medical imaging models for specific applications, such as early-stage tumor detection. This will drastically reduce the time and resources required to train a robust model by leveraging collective intelligence without the legal overhead of a centralized data lake.