# Adversarial Machine Learning with Gene Expression for Major Depressive Disorder

**Setareh Akbari ***
University of Tulsa, Tulsa, OK, USA

**Jamie Li**
University of Tulsa, Tulsa, OK, USA

**Brett McKinney**
University of Tulsa, Tulsa, OK, USA

## Abstract

Data sharing is essential for the reproducibility and integrity of both clinical and basic research. The ability to share data among researchers facilitates the validation of findings, fosters collaboration, and accelerates scientific discovery. However, one of the significant challenges in data sharing is the need to maintain the privacy of patients or study participants. To address these privacy concerns, privacy-preserving techniques and generative adversarial machine learning have emerged as powerful tools. These methods can modify or simulate data in a manner that protects participant privacy while retaining the essential characteristics necessary for analysis. By introducing controlled noise or generating synthetic datasets that mimic real data, researchers can share information without risking the exposure of personal identifiers.

Gene expression data is generally considered more privacy-resilient compared to data from genome-wide association studies (GWAS), primarily because gene expression datasets are inherently noisier. This noise acts as a buffer, making it more difficult to trace back to individual participants, thus providing a layer of protection for sensitive information. However, demographic data, which often accompanies gene expression data, can still pose privacy risks and must be handled with caution.

Beyond just protecting privacy, the use of generative synthetic data from gene expression datasets can enhance the analytical capabilities of researchers. By generating additional data points that capture the statistical properties of real samples, these techniques can improve the detection of subtle statistical effects that might otherwise go unnoticed due to limited sample sizes. This is particularly relevant in areas like mental health research, where distinctions between groups, such as major depressive disorder and healthy controls, can be nuanced and challenging to identify at the expression level.

In our study, we employ artificial and real gene expression data, utilizing adversarial machine learning techniques to generate simulated samples that capture the critical properties of real datasets. This approach not only ensures the confidentiality of the original samples but also allows us to augment our dataset. We specifically test the effectiveness of these simulations to improve classification accuracy between individuals diagnosed with MDD and healthy controls. By evaluating the performance of models trained on both real and augmented datasets, we aim to demonstrate that synthetic data can play a pivotal role in enhancing the robustness of our findings while safeguarding participant privacy.

## Keywords

Adversarial Machine Learning, Gene Expression, Privacy-Preserving Techniques, Synthetic Data, Major Depressive Disorder.