



















Conditional Generative Adversarial Networks













Differential Privacy GAN

Reverse engineering medical records from neural networks Reconstruction of privacy-sensitive data from protected

templates The secret sharer: evaluating and testing unintended memorization in neural networks

Generating Synthetic Data

Casey Green's GAN using differential privacy Fake patient data Clear privacy guarantees







