

Report

Written by Amalie Dyrberg Holm (amdh), Lambda Nørbjerg (emno), and Mikkel Bistrup Andersen (mbia).

GDPR Reflections

A written report reflecting on the questions in “1”, Reflect on this scenario in the context of the GDPR: What are the potential issues in having the hospital store plaintext private data provided by patients even if they have consented to participate on the experiment and have their data processed? Would these issues be solved by removing the patients’ names from their data before storing it? What are the remaining risks in using Federated Learning with Secure Aggregation as suggested?

Adversarial model

describing the adversarial model you are working on,

Building blocks of the solution

describing the building blocks of your proposed solution,

Combination

how they are combined in your final solution and

Security guarantees

why they guarantee security against the adversary you describe.