Chapter 10
Federated Generative Frameworks for Adaptive Privacy Preservation in Healthcare Systems

Yalla Anitha
http://orcid.org/0009-0001-6285-0778
SR University, India

R. VijayaPrakash
http://orcid.org/0000-0003-2177-5350
SR University, India

R. S. Dubey
http://orcid.org/0000-0003-1152-7257
S.B. Jain Institute of Technology Management and Research, India

ABSTRACT

This chapter details an architecture for privacy-preserving interoperability to enable remote healthcare institutions to collaborate safely, supported by federated learning and generative modelling. It overcomes the direct sharing of sensitive medical records through adaptive privacy control algorithms for the realization of representative datasets. The proposed solution of joint local model training over heterogeneous data, statistically consistent synthetic data augmentation, and dynamic privacy governance at the data generation layer is designed to address three fundamental challenges: data heterogeneity, inference attacks, and legal boundaries between institutions. This chapter covers the operational modes, governance issues, and system components that allow real-world implementation, while addressing

DOI: 10.4018/979-8-3373-7426-0.ch010

important ethical and technological issues such as model robustness, scalability, and synthetic data authenticity. The framework enables practical solutions that support large-scale medical analytics without privacy-violating compromise during collaborative healthcare workflows.

INTRODUCTION

As they continue to get digital, hospitals, research centres, and clinical networks are producing and handling large amounts of clinical data in various forms. Medical imaging, clinical decision support based on data and electronic health records are improving the results that patients once believed they were not capable of achieving. The healthcare data is extremely sensitive and is prone to tight institutional, privacy, and regulatory controls. Specifically, the paradigms of traditional centralised data analytics no longer fit well in multi-institutional environments, where a variety of data governance needs need to be balanced.

This has made the decentralised means of analysis more popular which are able to bypass these constraints. Federated learning has become a potentially promising decentralized paradigm that allows collaborative model learning and retains institutional data locally. In federated systems, the participating institutions exchange model updates instead of direct patient data hence limited exposure of sensitive clinical information. However, parameter sharing alone does not fully address privacy risks, particularly in the presence of data heterogeneity, class imbalance, and disparities in institutional resources.

Recent advances in generative modelling offer complementary mechanisms to mitigate privacy risks while supporting analytical utility. They can create synthetic data that replicates more profound statistical features, but without disclosing any identifiable medical data. In such settings, synthetic data generation can reduce reliance on regulated data sharing, mitigate institutional bias, and address data scarcity.

This chapter outlines the theoretical and infrastructural underpinnings of federated-generative frameworks for privacy-preserving healthcare analytics and discusses some of the implementation, ethical and regulatory challenges of scaling these systems up to a multi-institutional level.

Chapter Contributions

Defines adaptive privacy control in federated–generative healthcare systems
Identifies concrete privacy risks and operational trade-offs in multi-institution analytics