Chapter 14
Federated Learning for Healthcare Data Privacy and Security: From EHRs to Personalized Medicine

S. Aarthi
http://orcid.org/0009-0006-9064-2091
Marwadi University, Rajkot, India

Jaypalsinh A. Gohil
http://orcid.org/0000-0003-0925-6646
Marwadi University, Rajkot, India

ABSTRACT

Federated Learning (FL) represents a revolutionary approach to achieving privacy-preserving intelligence in healthcare by enabling multi-institutional AI collaboration without sharing sensitive patient data. This study investigates FL's potential to enhance data privacy, security, and interoperability across Electronic Health Records (EHRs), medical imaging, genomics, and personalized medicine. By integrating Differential Privacy, Homomorphic Encryption, and Secure Multi-Party Computation, the proposed framework ensures HIPAA and GDPR compliance while maintaining model accuracy and trust. The research highlights how FL mitigates risks of data breaches, fosters ethical AI-driven healthcare ecosystems, and supports precision diagnostics, predictive analytics, and individualized treatment through secure, scalable, and decentralized data governance.

DOI: 10.4018/979-8-3373-7426-0.ch014

INTRODUCTION

The application of Artificial Intelligence (AI) unlocks new possibilities for health improvement in the UK through improved diagnosis, treatment planning, and treatment management systems. The training of AI models in medicine is heavily dependent on voluminous sets of patient-sensitive information, which raises multiplicity of privacy risks while generating security problems. Federated Learning (FL) thus provides a solution to AI model training for hospitals and clinics with collaborative development without exposing raw patient data. Through distributed management healthcare providers maintain patient confidentiality since medical advances derive from shared information rather than record disclosure. Secure data processing within FL systems becomes more robust due to the implementation of privacy-protecting features including Differential Privacy (DP) and Homomorphic Encryption (HE) and secure multi-party computation (Xu et al., 2021a). The advancement of medical technology serves as an essential component of healthcare because it allows organizations to meet their ethical implementation of AI system requirements under HIPAA and GDPR. The healthcare organizations which can relate FL to the current AI transformers as analytical tools are able to create new technologies of medical imaging and drug discovery as well as secured Electronic Health Records (EHR) processing.

AI in Healthcare and Privacy

The medical care is subject to radical changes due to the presence of AI that helps the doctor with the diagnosis of the disease and improves the analytical abilities in health and treatment planning. Deep learning technology and natural language processing protocol-based programs are used to automatize the analysis of medical images alongside EHR and genomic data to construct improved clinical decisions and personalized medical care towards patients. In (Chelani et al., 2024a), wearable devices along with remote monitoring solutions allow providing patients with medical assistance instantly and reducing the number of visits to healthcare facilities to better access the facility. The implementation of AI healthcare applications requires the volumes of big data on the part of patients, and, at the same time, it creates several security issues and privacy concerns along with dilemmas of ethical use. The conventional centralized artificial intelligence system requires that all patient records be stored in one storage center since this system will expose health records to security attacks in addition to providing access to unauthorized users and misuse. Medical utility knowledge is developed through privacy protecting methods that prevent the medical information of the patient to be under scrutiny. The advantages of the FL technology are described in Figure 1, so it is the decentralized modeling of AI and