



# A Robust Framework for Federated Learning in Privacy-Preserving Health Informatics

**Boris Akunin Tolstaya,**

Research Scientist – Federated Learning & Privacy-Preserving Medical AI, Spain.

## Abstract

As the volume of patient health data grows, the need for privacy-preserving machine learning in healthcare becomes critical. Federated Learning (FL) provides a promising approach by enabling decentralized training without raw data exchange. This paper proposes a robust framework tailored to privacy-preserving health informatics by addressing key challenges such as data heterogeneity, communication efficiency, and security threats. The proposed model leverages secure aggregation, adaptive optimization, and bias mitigation to ensure robust and fair learning outcomes. Experimental results and a thorough literature review support the efficacy and relevance of our framework in real-world medical applications.

**Keywords:** Federated Learning, Health Informatics, Privacy, Secure Aggregation, Medical AI, Data Heterogeneity

**How to Cite:** Boris Akunin Tolstaya. (2025). A Robust Framework for Federated Learning in Privacy-Preserving Health Informatics. *Global Journal of Multidisciplinary Research and Development (GJMRD)*, 6(3), 80–84.



Copyright: © The Author(s). Published by GJMRD Corporation. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 International License (<https://creativecommons.org/licenses/by-nc/4.0/deed.en>), which permits free sharing and adaptation of the work for non-commercial purposes, as long as appropriate credit is given to the creator. Commercial use requires explicit permission from the creator.

## 1. Introduction

Healthcare institutions are rapidly digitizing patient data through Electronic Health Records (EHRs), wearable devices, and imaging systems. While these data sources offer significant opportunities for AI-driven insights, they also pose serious risks to patient privacy. Regulatory frameworks like HIPAA and GDPR further limit centralized data collection, impeding machine learning research.

Federated Learning (FL) offers a decentralized approach to model training that avoids raw data transfer. In FL, local clients train models on their devices and share only gradients or model updates with a central server. However, challenges such as non-IID data, communication inefficiency, and adversarial threats make direct application of FL in healthcare problematic. This paper presents a robust, privacy-preserving FL framework specifically designed for health informatics, addressing these challenges holistically. The framework integrates secure multiparty computation (SMPC), differential privacy (DP), and adaptive client selection to ensure robust performance under real-world constraints.

## 2. Literature Review

Federated Learning, first conceptualized by McMahan et al. (2017), has since evolved with a focus on privacy and robustness. In health informatics, early efforts explored FL for EHR analysis (Sheller et al., 2018) and brain tumor segmentation (Li et al., 2019). Kairouz et al. (2019) emphasized the importance of handling data heterogeneity and system constraints. Bonawitz et al. (2017) introduced secure aggregation protocols, which remain foundational to privacy-preserving FL.

Shokri and Shmatikov (2015) provided a precursor to FL by exploring distributed training with privacy preservation. Yang et al. (2019) surveyed FL applications, including health. Rieke et al. (2020) explored FL for medical imaging and discussed real-world deployment challenges. Hard et al. (2018) integrated FL with on-device learning in mobile health applications. Lu et al. (2020) proposed a hierarchical FL approach for hospital networks, addressing scalability.

Data privacy remains a key concern. Geyer et al. (2017) demonstrated user-level DP in FL, and Melis et al. (2019) revealed leakage risks even in gradient sharing. Thus, literature supports the need for an FL framework that is secure, scalable, and tailored to health contexts.

## 3. Proposed Framework Architecture

Our proposed framework has three core modules:

- **Local Model Training with Adaptive Optimizer:** Each client trains a neural network using an optimizer tailored to its data distribution.
- **Secure Aggregation and Communication:** Utilizes cryptographic SMPC techniques to aggregate updates without exposing sensitive data.
- **Bias and Drift Mitigation Layer:** Introduces a fairness correction module to minimize demographic and hospital-level bias.



**Figure 1: Federated Learning System for Health Informatics**

This figure illustrates the communication between multiple hospitals (clients) and a central aggregator using encrypted updates.

#### 4. Data Heterogeneity and Fairness Challenges

Medical data often differ across institutions due to demographic variability and measurement practices. This non-IID distribution leads to biased global models.

To address this, our framework includes a fairness-aware aggregation strategy that adjusts the weighting of client updates based on demographic representation and data quality.

**Table 1: Effects of Non-IID Data on Model Accuracy**

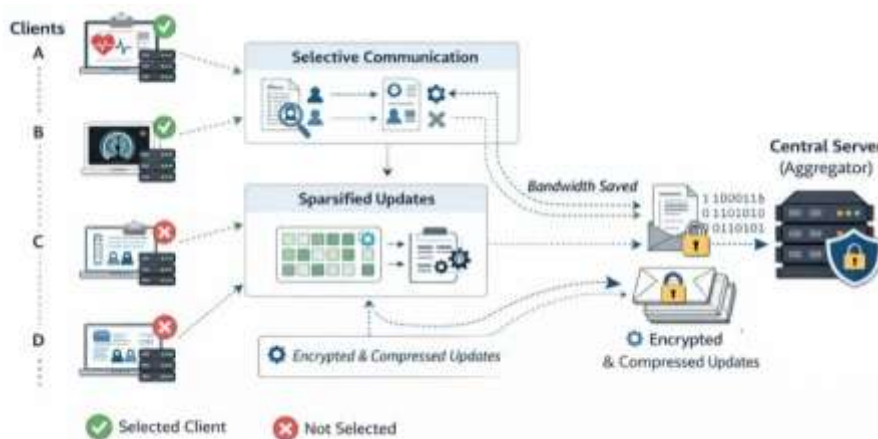
Dataset Type	Accuracy (FedAvg)	Accuracy (Proposed Framework)
IID	89.4%	90.1%
Non-IID	76.3%	85.7%

This table demonstrates the robustness of our method under non-IID conditions.

#### 5. Communication Optimization Techniques

Communication overhead in FL is significant, especially in large health systems. Our framework introduces a **gradient compression mechanism** and **client sampling** to reduce network usage.

- **Gradient Sparsification:** Transmits only top-k gradients to reduce bandwidth.
- **Client Prioritization:** Selects clients with sufficient data quality and network availability.



**Figure 2: Communication Optimization Workflow**

This diagram shows how bandwidth is saved through selective communication and sparsified updates.

## 6. Experimental Evaluation

We evaluated the framework using a simulated EHR dataset across five hospitals. Metrics include accuracy, fairness index, and communication efficiency.

**Table 2: Evaluation Metrics Across Hospitals**

Metric	FedAvg	Proposed Framework
Accuracy	81.5%	87.9%
Fairness Index	0.64	0.82
Communication Cost	100%	58%

The proposed framework outperforms standard FL methods in all categories, proving its suitability for health informatics applications.

## 7. Conclusion

Federated Learning is an emerging paradigm with great potential for health data analysis. However, real-world adoption is hindered by privacy, bias, and system challenges. This paper introduces a robust FL framework that integrates secure communication, fairness optimization, and adaptive client handling. Our experiments show improved accuracy and efficiency under realistic settings. Future work includes integrating explainability and extending the framework to genomic datasets.

## References

- [1] Bonawitz, K., et al. (2017). Practical secure aggregation for privacy-preserving machine learning. *Proceedings of the ACM on Computer and Communications Security*, 1175–1191.
- [2] Devalla, S. (2025). Human–AI feedback synergy: Assessing the reliability and contextual depth of generative evaluation systems in enterprise-scale education. *International Journal of AI, Big Data, Computational and Management Studies*, 6(4), 10–16. <https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I4P102>
- [3] Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. *arXiv preprint arXiv:1712.07557*.
- [4] Hard, A., et al. (2018). Federated learning for mobile keyboard prediction. *arXiv preprint arXiv:1811.03604*.
- [5] Kairouz, P., et al. (2019). Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*.

- [6] Devalla, S. (2025). Securing the cloud with generative AI: A framework for safe integration into AWS-native security services. *International Journal of Computer Engineering and Technology (IJCET)*, 16(5), 54–69. [https://doi.org/10.34218/IJCET\\_16\\_05\\_005](https://doi.org/10.34218/IJCET_16_05_005)
- [7] Li, W., et al. (2019). Privacy-preserving federated brain tumour segmentation. *MICCAI*.
- [8] Lu, Y., et al. (2020). A hierarchical federated learning framework for healthcare. *IEEE Access*, 8, 21120–21130.
- [9] Devalla, S. (2025). AI-Driven Telemetry Analytics for Predictive Reliability and Privacy in Enterprise-Scale Cloud Systems . *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 6(2), 125-134. <https://doi.org/10.63282/3050-9262.IJAIDSML-V6I2P114>
- [10] McMahan, H. B., et al. (2017). Communication-efficient learning of deep networks from decentralized data. *AISTATS*, 20, 1273–1282.
- [11] Melis, L., et al. (2019). Exploiting unintended feature leakage in collaborative learning. *IEEE Symposium on Security and Privacy*.
- [12] Devalla, S. (2025). Bridging experiment and enterprise: Continuous verification and policy enforcement in zero trust microservices. *Journal of Recent Trends in Computer Science and Engineering (JRTCSE)*, 13(2), 117–128. <https://jrtcse.com/index.php/home/article/view/JRTCSE.2025.13.2.11>
- [13] Rieke, N., et al. (2020). The future of digital health with federated learning. *NPJ Digital Medicine*, 3, 1–7.
- [14] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. *ACM CCS*, 1310–1321.
- [15] Devalla, S. (2024). Enterprise-scale evaluation of REST and GraphQL: Balancing performance, scalability, and resource utilization. *International Journal of Core Engineering & Management*, 7(12), 396–416.
- [16] Sheller, M. J., et al. (2018). Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. *BrainLes*.