Dean&Francis
ISSN 2959-6157

# Progress in Applying Federated Learning to Cross-Institutional Medical Data Collaboration

**Shichen Zhang**

School of Beijing Dublin International College, Beijing University of Technology, Beijing, China
Corresponding author: shichen.zhang@ucdconnect.ie

**Abstract:**

The advancement of healthcare informatization has resulted in the exponential growth of patient data stored across various hospitals, laboratories, and clinical centers, properly integration and analysis of this data and use it for machine learning can help make medical processes more efficient. However, privacy regulations and institutional silos pose substantial barriers to collaborative research and centralized model training. Here, Federated Learning (FL) has surfaced as an innovative distributed learning approach, as it empowers institutions to jointly build models while safeguarding raw data privacy. This review outlines FL's fundamentals and highlights its applications across multiple healthcare domains, including medical image analysis, clinical outcome prediction, and wearable health monitoring. The fundamental FL designs (horizontal FL, vertical FL, and split FL learning) and privacy-enhancing methods (safe aggregation, homomorphic encryption, and differential privacy) are discussed. Additionally, we also examine recent advances in adaptive privacy mechanisms, asynchronous updates and explainable AI to support clinical integration. The study concludes with a discussion of current limitations and future research directions, such as multimodal FL, personalized modeling, and edge-based computing.

**Keywords:** Federated learning; Medical data collaboration; Privacy-preserving machine learning.

## 1. Introduction

As the informatization process of medical industry is speeding up, a large amount of medical data has accumulated in hospitals, clinics and laboratories. This has led to the formation of siloed local nodes, which severely affected the progress of inter-instructional cooperation and large-scale model training. To make matters more difficult, confidentiality statutes such as HIPAA and GDPR give strict prohibitions on exchanging patients' health records, making centralized data aggregation even less feasible. To solve these

ISSN 2959-6157

challenges, Federated Learning (FL), came into being. FL actually is a style of framework of machine learning, which is non-centralized [1]. FL enables institutions to perform local model training while exchanging only parameters and updates, keeping the original data confidential. This mechanism of "keeping data locally, sharing models globally" takes into account both model performance and data privacy requirements, providing a possible way for medical collaboration. In the medical field, FL has shown wide application value. First is the Medical image analysis. FL can enhance the model generalizability without sharing sensitive images by enabling multi-institutional collaboration. Besides, Clinical outcome prediction is a kind of Federated models trained by EHR data from multiple hospitals have shown that they have strong ability to predict COVID-19 mortality and other conditions [2]. Last but not least, in order to preclude the personal information of patient from being exposed when the continuous about health monitoring, Internet-of-medical-things (IoMT) data technology comes up. This kind of local training of wearable devices or sensors is a suitable solution.

In recent years, many studies have confirmed that FL can still show performance similar to centralized training while ensuring the security of private data [3]. In addition, the platform and algorithms continue to mature, including privacy-enhancing mechanisms as demonstrated by differential privacy, homomorphic encryption, and secure aggregation, which effectively deal with non-IID data, communication costs, and potential attack risks. This review seeks to present an extensive survey on the applications of federated learning within the healthcare domain: First, I will present the core concepts of FL and emphasize its unique value in healthcare applications. Then, I will analyze existing technical systems and deployment architectures—covering horizontal and vertical FL, split learning, and privacy-preserving techniques—and review key use cases. Finally, I will present development trends based on the current status of FL, such as multimodal FL, personalized modeling, incentive mechanisms, and persistent clinical deployment barriers. By combining theory with practice, this overview provides a valuable roadmap for academic researchers and practitioners to guide and advance the safe and effective application of FL in healthcare.

# 2. Federated Learning Fundamentals & Its Value in Medicine

## 2.1 What Is Federated Learning

Federated learning (FL) fundamentally follows the idea that "data remains local, while the model gets shared [1]", this can promote collaboration among institutions to protect privacy. In a typical FL cycle: a primary server sends a centralized model to clients, and then every client can optimize the model on locally measurements, returning nothing except model updates. Finally, these models will be pooled into a revamped form, improved consolidated model. This approach effectively addresses two major obstacles in making progress on medical issues: one hindrance among is to protect patients' privacy, and another one is how to manage data heterogeneity owing to differences in imaging protocols, device types, and patient demographics.

## 2.2 Core Algorithms & Privacy Enhancements

Federated Averaging (FedAvg) is the cornerstone algorithm of FL. This algorithm allows clients to train several times locally before sending compressed and aggregated model updates to the server. This approach has greatly reduced communication costs and, also can achieve results comparable to centralized training.

## 2.3 Medical Applications & Impact

### 2.3.1 Medical Image Analysis

Large and diverse imaging datasets are essential for model development. However, due to the privacy laws, sharing raw images is often not practical. But thanks to the mechanism of federated learning, institutions can collaborate on training without exchanging data. This kind of technology enables multi-center CT, MRI, and X-ray model training while ensuring data security.

### 2.3.2 Medical Applications & Impact

One common example is the EXAM model, which predicts the oxygen requirement of COVID-19 patients using data from 20 healthcare facilities worldwide. In predicting prognostic outcomes with in 24 and 72 hours following a patient's initial emergency department visit, the EXAM model achieved an average discrimination index (AUC) exceeding 0.92. This demonstrating exceptional discriminative of EXAM. This result underscores the model's high reliability in terms of predictive accuracy. Compared to models developed solely on data from a single research center, EXAM integrates data from multiple participating centers, resulting in a 16% improvement in the average AUC across all centers, significantly enhancing the model's external validity. Furthermore, the model's transferability improved by approximately 38%, indicating robust applicability and consistency across diverse clinical contexts and patient cohorts [2]. This data increase validates and demonstrates how Federated Learning can markedly

enhance predictive performance while safeguarding patient privacy.

## 3. Existing technical system of federated learning in medical scenarios

After outlining the paradigm of FL, it is now time to examine in detail how these architectures and privacy mechanisms can be assembled into practical systems suitable for clinical applications.

### 3.1 System Architecture and Paradigm Classification

First, there are three main architectures for federated learning across healthcare institutions:
Horizontal federated learning is utilized when different hospitals occupy a common feature space (e.g., demographics, lab results, images) but manage different patient populations. This type of federated learning enhances statistical power as it preserves the confidentiality of the original data [1].
Vertical federated learning complements this setting by linking complementary feature sets of overlapping patients (e.g., electronic health records (EHR) plus genomics) and enabling richer models through feature fusion [4].
Split learning divides the neural network itself between the client and the server. It exchanges intermediate activation values instead of raw inputs, which makes it a privacy-focused architectural alternative that is particularly suitable for vertically divided hospital systems [5].

### 3.2 Privacy and Security Mechanisms

Having outlined architectures, we turn next to mechanisms safeguarding patient privacy: Differential privacy introduces calibrated noise into model updates, preserving utility while limiting the model from being a channel for leaking any personally sensitive information in the training dataset [6]. Secure aggregation protocol ensures that only aggregated model parameters are visible to the coordination server [7]. Homomorphic encryption and multi-party computation support computation on encrypted data, but the computational cost is high [8]. These combined techniques support privacy assurance in the context of healthcare network identity (FL) and are widely described in various frameworks.

### 3.3 Platform Support

To enable the implementation of Federated Learning (FL), several open source platforms provide the necessary tools: MedPerf benchmarks can distribute medical AI models without centralizing data; TensorFlow Federated provides an extensible research framework, which supports FL simulation for horizontal and vertical setups; FATE (Federal AI Technology Enabler) has specially developed three technologies, namely secure aggregation, HE and MPC, for healthcare applications to support safe and stable actual production use. Despite these advances, integration with hospital IT systems remains non-trivial due to interoperability challenges, regulatory requirements, and coordination of clinical workflows.

### 3.4 Using Cases

Application Examples Federated learning has been successfully applied to multiple healthcare-related segments and has brought tangible improvements to the work in this field: In medical imaging for diagnostic purposes, employing a multi-center federated learning approach has effectively enhanced breast cancer identification, lung nodule recognition on CT scans, as well as retinal pathology classification. Compared with single-center training, the typical value of model AUC has increased by about 5-10% [9]; in the field of clinical outcome prediction, federated learning models have been successfully used to predict COVID-19 prognosis (such as mortality, ICU admission rate), and AUC>0.80 has been achieved in multi-hospital studies [10]; in wearable health monitoring, datasets associated with electronic health records (EHR) and derived from the Internet of Things (IoT) (such as electrocardiograms and psychological signals) have achieved federated detection of mental health status and arrhythmias, with an F1 score of>0.85 [11].

### 3.5 Comparative Evaluation

Comparative Evaluation Studies have shown that horizontal, vertical, and split FL differ in performance, communication cost, and privacy assurance: horizontal FL generally provides the highest AUC (0.85-0.92) with moderate communication cost [12]; vertical FL increases feature richness and improves performance by about 3%, but encryption overhead is relatively higher [1]; split learning minimizes the exchange of raw data, but the accuracy may vary (up to 8%) depending on the location of the slice. The effectiveness of the model is usually measured by accuracy, AUC, F1 score, number of communication rounds, bandwidth consumption, and formal privacy proofs [4]. Current benchmarks emphasize that no FL method is universally optimal, and deploying FL must balance data heterogeneity, privacy requirements, and system constraints.

## 4. Future Trends in Medical Federated Learning

However, despite the current positive development trend

ISSN 2959-6157

of the federated learning (FL) framework, there are still many challenges along the way.

### 4.1 Adaptive Differential Privacy

As mentioned above, adding noise is a guarantee to avoid leaking private data during model training. However, if noise is added blindly all the time, it will generate too much computational burden. Therefore, the research on adaptive differential privacy came into being. This method does not simply add noise, but adapts the privacy parameters based on the sensitivity of each dataset. Through a lightweight encryption protocol tailored for hospitals, the computational burden can be greatly reduced without exceeding the regulatory scope [13].

### 4.2 Beyond Batch Model Updates

As the scale of model training data increases, batch sending and receiving models can no longer meet the needs. To solve this problem, methods such as gradient compression, hierarchical aggregation, and asynchronous client updates are booming. Furthermore, it's intriguing to note that recently conducted research has demonstrated that these modifications may even enhance model convergence when dealing with identically distributed (IID) data, particularly when paired with class imbalance techniques [14].

### 4.3 Explanation and Standardization by Design

Gaining the trust of clinicians is essential to advancing the integration of federated learning models into medical practice. Therefore, explainable logical reasoning tools (such as local SHAP or Grad-CAM) are becoming essential rather than optional. In addition, interoperability standards consistent with the ontology are gaining more and more attention to make real-world deployment possible rather than just an ideal aspiration [13].

### 4.4 Cutting-edge technology: basic model and edge elastic computing

Combining the joint fine-tuning of basic models in the healthcare field with elastic edge-based computing on hospital nodes or devices is a possible direction. This direction is expected to reduce latency, improve autonomy, and truly realize clinical applications - although it also complicates trust, explainability, and architecture.

## 5. Conclusion

In summary, Federated learning (FL) facilitates joint model development among diverse healthcare entities while shielding private patient information, effectively solving the data silo problem and promoting inter-institutional cooperation under strict privacy-preserving legal frameworks. It augments predictive capability without compromising the security of local dataset, which highlights its key value in modern healthcare. We not only reviewed the core architecture (e.g., horizontal learning, vertical learning, and split learning) of federated learning but also a broad of different privacy-protection schemes. Notable applications include medical imaging (e.g., breast cancer, CT scans), clinical outcome prediction (e.g., COVID-19 prognosis), and wearable-based health monitoring, all of which have shown improvements in model generalization and accuracy.

Despite these advances, significant challenges remain. Data heterogeneity between clients can lead to statistical biases and related issues of non-IID, which can affect model convergence. In addition, federated learning systems consume a lot of computing resources and bandwidth, which limits their application in clinical settings. Complying with evolving regulatory frameworks, ensuring deployments fit hospital workflows, and earning clinician trust also become socio-technical hurdles. Looking ahead, future efforts should focus on:

· Multimodal integration: Incorporating electronic health record (EHR), imaging, genomics, and wearable device data into federated learning (FL) to enhance diagnostic capabilities.

· Personalized federated learning: Tailoring models to institution-specific distributions for meta-learning or personalized aggregation.

· Standardized security assessments: Creating benchmarks and audit protocols to safeguard the privacy, robustness, and performance of federated learning systems.

· Interpretability and interoperability: Embedding interpretable modules that meet clinical standards to ensure transparency and seamless clinical application.

· After addressing these issues, federated learning can develop into a robust, secure, and tightly clinically integrated technology. Such advances hold the promise of decentralized AI, which will have a real impact on the entire healthcare ecosystem while protecting patient privacy.

## References

[1] Guan, H., Yap, P.T., Bozoki, A. & Liu, M., 2024. Federated learning for medical image analysis: A survey. arXiv preprint arXiv:2306.05980.

[2] Dayan, I., Roth, H., Zhong, A., Gilbert, F.J., Li, Q. & Flores, M.G., 2021. Federated learning for predicting clinical outcomes in patients with COVID-19. Nature Medicine, 27(10), pp.1735–1743.

[3] Joshi, H. & Joseph, S., 2025. Standardization and interoperability: Federated learning's impact on EHR systems

and health informatics. Advances in Health Information Science and Practice, 1(1), Article UBYM3803.

[4] Yang, T., Yu, X., McKeown, M.J. & Wang, Z.J., 2024. When federated learning meets medical image analysis: A systematic review with challenges and solutions. APSIPA Transactions on Signal and Information Processing, 13, e38.

[5] Nampalle, K.B., Singh, P., Narayan, U.V. & Raman, B., 2023. Vision through the veil: Differential privacy in federated learning for medical image classification. arXiv preprint arXiv:2306.17794.

[6] Zhang, F., Kreuter, D., Chen, Y., Dittmer, S., Tull, S., Shadbahr, T., BloodCounts! consortium, Preller, J., Rudd, J.H.F., Aston, J.A.D., Schönlieb, C.-B., Gleadall, N. & Roberts, M., 2024. Recent methodological advances in federated learning for healthcare. Patterns, 5, 101006.

[7] Li, K., Liang, Y., Yuan, X., Ni, W., Crowcroft, J., Yuen, C. and Akan, O.B., 2024. A novel framework of horizontal-vertical hybrid federated learning for EdgeIoT. arXiv preprint arXiv:2410.01644.

[8] Ali, M.S., Ahsan, M.M., Tasnim, L., Afrin, S., Biswas, K., Hossain, M.M., Ahmed, M.M., Hashan, R., Islam, M.K. & Raman, S., 2024. Federated learning in healthcare: Model misconducts, security, challenges, applications, and future research directions – A systematic review. arXiv preprint arXiv:2405.13832.

[9] Rehman MHU, Hugo Lopez Pinaya W, Nachev P, Teo JT, Ourselin S, Cardoso MJ. Federated learning for medical imaging radiology. Br J Radiol. 2023 Oct;96(1150):20220890.

[10] Bai, X., Wang, H., Ma, L., Xu, Y. et al. Advancing COVID-19 diagnosis with privacy-preserving collaboration in artificial intelligence. arXiv preprint arXiv:2111.09461.

[11] Ankolekar, A., Boie, S., Abdollahyan, M. et al. Advancing breast, lung and prostate cancer research with federated learning. A systematic review. npj Digit. Med. 8, 314 (2025).

[12] Roth, H.R., Chang, K., Singh, P., Neumark, N. et al. Federated learning for breast density classification: A real-world implementation. In: Albarqouni, S. et al. (eds.) Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning. Lecture Notes in Computer Science, vol. 12444. Cham: Springer, pp. 109–121.

[13] Parampottupadam, S., et al., 2025. Inclusive, Differentially Private Federated Learning for Clinical Data. arXiv [preprint] arXiv:2505.22108v1.

[14] Oh W, Nadkarni GN. Federated Learning in Health care Using Structured Medical Data. Adv Kidney Dis Health. 2023 Jan;30(1):4-16.