What Is the Role of Federated Learning in Healthcare Privacy?

Rasit Dinc

Rasit Dinc Digital Health & AI Research

Published: April 28, 2024 | Healthcare Data Privacy and Security

DOI: 10.5281/zenodo.17998397

Abstract

In the era of big data, the healthcare industry is increasingly leveraging artificial intelligence (AI) and machine learning (ML) to improve patient outcomes...

What Is the Role of Federated Learning in Healthcare Privacy?

Author: Rasit Dinc

In the era of big data, the healthcare industry is increasingly leveraging artificial intelligence (AI) and machine learning (ML) to improve patient outcomes and drive medical innovation. However, the use of sensitive patient data raises significant privacy concerns. Federated learning (FL) has emerged as a promising solution to this challenge, enabling the development of robust AI models without compromising patient privacy. This article explores the role of federated learning in healthcare privacy, its benefits, challenges, and the governance frameworks required for its successful implementation.

The Privacy-Preserving Power of Federated Learning

Federated learning is a decentralized machine learning approach that allows multiple organizations to collaboratively train a shared model without exchanging their raw data [1]. In the context of healthcare, this means that hospitals and research institutions can work together to build powerful AI models for tasks such as disease diagnosis, drug discovery, and personalized medicine, all while keeping sensitive patient information securely within their own firewalls. This is a significant departure from traditional machine learning methods, which require data to be centralized in a single location, creating a single point of failure and increasing the risk of data breaches.

A recent study published in *Nature* demonstrates the effectiveness of combining federated learning with transfer learning for medical image classification [1]. The researchers developed a novel adaptive aggregation method that dynamically switches between different learning algorithms to optimize model convergence and enhance privacy. Their findings show that

this approach is a scalable, robust, and secure solution for real-world medical diagnostics, allowing healthcare institutions to train highly accurate models without compromising patient data.

Benefits of Federated Learning in Healthcare

The adoption of federated learning in healthcare offers several key benefits:

| Benefit | Description | | :--- | :--- | | **Enhanced Privacy** | Patient data remains at the local institution, significantly reducing the risk of data breaches and ensuring compliance with data protection regulations such as GDPR and HIPAA. | | **Improved Model Accuracy** | By training on diverse datasets from multiple institutions, federated learning models can achieve higher accuracy and generalizability than models trained on a single dataset. | | **Increased Collaboration** | Federated learning facilitates collaboration between healthcare organizations, enabling them to pool their resources and expertise to tackle complex medical challenges. |

Challenges and Mitigation Strategies

Despite its numerous benefits, the implementation of federated learning in healthcare is not without its challenges. One of the main concerns is the risk of model inversion and membership inference attacks, where malicious actors could potentially infer sensitive information from the model's updates. To mitigate these risks, researchers have proposed several strategies, including:

Secure Multi-Party Computation (SMPC): *This technique involves splitting model updates into multiple secret shares, making it impossible for any single party to reconstruct the original data [2].* **Differential Privacy:** This method adds a small amount of noise to the data or model updates, which helps to protect the privacy of individual patients without significantly impacting the model's accuracy [3].

Another significant challenge is the lack of standardized governance frameworks for federated learning in healthcare. A scoping review published in *npj Digital Medicine* highlights the need for robust data governance frameworks that include procedural, relational, and structural mechanisms [2]. The authors emphasize the importance of establishing clear roles and responsibilities, implementing strong security measures, and ensuring ethical oversight to ensure the responsible use of health data.

The Path Forward: Governance and Collaboration

For federated learning to reach its full potential in healthcare, it is essential to establish clear governance frameworks and foster a culture of collaboration. This includes developing standardized data formats and protocols, as well as creating ethical guidelines for the use of federated learning in medical research. By working together, healthcare organizations, researchers, and policymakers can create a trusted ecosystem for federated learning that accelerates medical innovation while protecting patient privacy.

In conclusion, federated learning represents a paradigm shift in how we approach data privacy in healthcare. By enabling collaborative research

without compromising patient data, federated learning has the potential to unlock new insights and drive significant advancements in medicine. However, to realize this potential, it is crucial to address the associated challenges and establish robust governance frameworks that ensure the responsible and ethical use of this powerful technology.

References

[1] Haripriya, R., Khare, N. & Pandey, M. Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Sci Rep* **15**, 12482 (2025). https://doi.org/10.1038/s41598-025-97565-4

[2] Eden, R., Chukwudi, I., Bain, C. *et al*. A scoping review of the governance of federated learning in healthcare. *npj Digit. Med.* **8**, 427 (2025). https://doi.org/10.1038/s41746-025-01836-3

[3] Gu, X., Sabrina, F., Fan, Z., & Sohail, S. (2023). A review of privacy enhancement methods for federated learning in healthcare systems. *International Journal of Environmental Research and Public Health*, *20*(15), 6539.