Radiology: Artificial Intelligence

Privacy-Preserving Federated Learning and Uncertainty Quantification in Medical Imaging

Journal:	*Radiology: Artificial Intelligence*
Manuscript ID	RYAI-24-0637.R2
Manuscript Type:	Review
Manuscript Categorization Terms:	Supervised learning < Type of machine learning < 8. MACHINE LEARNING, Perception < Artificial neural network algorithms < Machine learning algorithms < 8. MACHINE LEARNING, Neural Networks < 2. MODALITIES/TECHNIQUES, Radiology-pathology integration < Integration < Application Domain < 8. MACHINE LEARNING

Privacy-Preserving Federated Learning and Uncertainty Quantification in Medical Imaging

Review Article

Keywords

Federated Learning, Medical Imaging, Privacy Preservation, Uncertainty Quantification, Review

Essentials

- Federated learning enables multi-institutional training of AI models on medical imaging data without direct data sharing, overcoming key privacy barriers while maintaining model performance.
- Despite privacy benefits, federated learning remains vulnerable to information leakage through gradient updates; privacy-preserving strategies such as differential privacy and homomorphic encryption reduce this risk but introduce accuracy and efficiency trade-offs.
- Uncertainty quantification in federated learning enhances model trustworthiness yet remains underutilized due to challenges posed by data heterogeneity and computational complexity.

Summary

This review article provides an in-depth analysis of the latest advancements in federated learning, privacy preservation, and uncertainty quantification in medical imaging. It also highlights current challenges and explores potential opportunities for improvement in these areas.

Abbreviations

AI:	Artificial Intelligence
ML:	Machine Learning
IID:	Independent and Identically Distributed
PFL:	Personalized Federated Learning
PPFL:	Privacy Preserving Federated Learning

Abstract

Artificial Intelligence (AI) has demonstrated strong potential in automating medical imaging tasks, with potential applications across disease diagnosis, prognosis, treatment planning, and post-treatment surveillance. However, privacy concerns surrounding patient data remain a major barrier to the widespread adoption of AI in clinical practice, as large and diverse training datasets are essential for developing accurate, robust, and generalizable AI models. Federated Learning offers a privacy-preserving solution by enabling collaborative model training across institutions without sharing sensitive data. Instead, model parameters, such as model weights, are exchanged between participating sites. Despite its potential, federated learning is still in its early stages of development and faces several challenges. Notably, sensitive information can still be inferred from the shared model parameters. Additionally, post-deployment data distribution shifts can degrade model performance, making uncertainty quantification essential. In federated learning, this task is particularly challenging due to data heterogeneity across participating sites. This review provides a comprehensive overview of federated learning, privacy-preserving federated learning, and uncertainty quantification in federated learning. Key limitations in current methodologies are identified, and future research directions are proposed to enhance data privacy and trustworthiness in medical imaging applications.

1 Introduction

Advances in artificial intelligence (AI), driven by deep learning and the availability of large datasets and computational resources, continue to transform medical imaging. AI models trained on radiological data, such as mammograms, CT scans, and MRIs, are poised to become invaluable tools in both clinical and research settings[1–3]. However, curating large, annotated, domain-specific datasets remains challenging, due to privacy regulations and other factors. Unlike conventional AI model development methods that require pooling data at a single location, federated learning enables decentralized model development without sharing data[4,5]. It allows for large-scale model training by sharing model gradient updates between sites rather than the training data. This enables multiple sites to act as clients and train a global model on the server, which is then shared with all sites.

Federated learning has the potential to address many challenges related to data sharing for AI model training in medical imaging[6]. However, it also presents unique challenges. First, data heterogeneity across different sites often violates the independent and identically distributed (IID) assumption, leading to issues such as poor model convergence, biased outcomes, and reduced generalization. These non-IID issues can stem from variations in imaging protocols, patient demographics, and disease prevalence across sites. Second, some studies have shown that private data can be extracted from the gradient updates communicated between federated learning sites[7]. Methods such as differential privacy[8] and homomorphic encryption[9] have been proposed to enhance communication security; however, there may be an inherent trade-off between privacy preservation and model performance[10]. The third challenge is uncertainty quantification, which involves measuring the AI's confidence in its predictions[11]. This is crucial for the trustworthiness and reliability of AI in clinical settings[11]. Almost all AI models based on deep neural networks require output calibration for accurate uncertainty quantification[12]. Due to the likelihood of non-IID data and potential class imbalance in datasets at client sites, traditional uncertainty quantification methods must be modified for federated learning models[13]. Federated learning, with strong privacy preservation and uncertainty quantification, has the potential to revolutionize medical imaging through development of generalizable, robust, and trustworthy AI models using large-scale multi-institutional datasets.

This work reviews state-of-the-art methods in federated learning, privacy-preserving federated learning (PPFL), and uncertainty quantification, outlining the potential of these advancements to transform medical imaging. The paper is organized as follows: Sections 2, 3, and 4 review federated learning, PPFL, and uncertainty quantification in federated learning, respectively. Section 5 covers the real-world applications of federated learning in medical imaging and summarizes the current challenges and opportunities. Figure 1 presents the organization of this review paper and Figure 2 presents the summary of the topics covered in this review. Readers are encouraged to refer to Supplementary material (section 7) for more detailed technical aspects of the various federated learning topics discussed in this paper. A GitHub repository with links to papers reviewed in this work is provided here: Awesome List. The primary contributions of this work include:

- A review of the current state-of-the-art federated learning methods, from the past five years, for learning from distributed data while addressing non-IID datasets, privacy-preservation requirements, and uncertainty quantification challenges.
- Exploration of five real-world use cases of federated learning in medical imaging and insights gained from these success stories. We also present current challenges in federated learning, PPFL, and uncertainty quantification related to medical imaging, along with potential opportunities for future research.

2 Federated Learning

Federated learning was originally proposed to train AI models on edge devices without exposing private data[14]. This led to a paradigm shift in how machine learning (ML) models could be trained on sensitive and private data in distributed settings. The original federated learning algorithm, FedAvg, trains local models on client data and sends gradient information to a central server to create a global model that, theoretically, can outperform all local models[14]. This section focuses on federated learning algorithms and presents state-of-the-art advancements. A summary of the topics is shown in Figure 3.

2.1 Federated Learning Algorithms - Characterization and Types

Federated learning can be classified as centralized or decentralized, depending on whether a central server is used to aggregate updates and construct the global model. Centralized federated learning is the more common approach, where a server orchestrates the learning process by collecting and combining client updates. In contrast, decentralized federated learning allows clients to communicate directly, which can be advantageous when a central server is impractical or undesirable due to privacy or connectivity constraints. Recently, personalized federated learning (PFL) has gained attention as an enhancement of traditional centralized federated learning[15]. PFL addresses the inherent data heterogeneity among clients, such as variations in data distributions (non-IID data), computational resources, and specific local requirements. Instead of creating a single global model, PFL focuses on developing models tailored to individual clients while still leveraging shared knowledge across federated learning sites. PFL models are generally trained within a centralized federated learning framework. Given their unique approach to personalization and adaptation in heterogeneous environments, the PFL algorithms reviewed in this paper are presented in a separate section. Table 1 summarizes all federated learning algorithms discussed.

2.2 Centralized Federated Learning

As illustrated in Figure 3A, centralized federated learning requires a dedicated central server for parameter aggregation and constructing the federated model. It is the most common form of federated learning implemented for various ML tasks. These algorithms offer technical advancements for (1) learning from distributed, heterogeneous, and non-IID data, (2) optimizing learning for both global and local models to avoid catastrophic forgetting, and (3) stabilizing training across

federated runs, locally and globally, to ensure model convergence. Notable centralized federated learning algorithms in recent years include FedProX[16], FedBN[17], FedGen[18], Federated Online Laplace Approximation (FOLA)[19], Train Convexify Train (TCT)[20], Federated Cross-Correlation and Continual Learning (FCCL)[21], and FedFA[22]. A technical summary of each algorithm can be found in supplement S1.

2.3 Decentralized Federated Learning

Decentralized federated learning implementations do not rely a central server to coordinate learning, as shown in Figure 3B[23–25]. Depending on the application, decentralized federated learning may enhance privacy and security while increasing robustness and fault tolerance by eliminating single points of failure. It also improves scalability by distributing workloads across the network. Decentralized federated learning methods such as Swarm Learning[23], ProxyFL[24], and Fog-FL[25] offer alternative approaches to conducting federated learning experiments when a centralized server is not practical. Additional information about these decentralized methods can be found in supplement S2.

2.4 Personalized Federated Learning (PFL) - Addressing Client Data Heterogeneity

In multi-institutional collaborations, patient demographics often vary widely across sites, a challenge amplified by geographic separation. These demographic differences can lead to substantial variation in datasets used to train a federated learning model across sites[26]. In some cases, this can prevent model convergence or lead to underperformance on local data. As shown in Figure 3C, PFL develops tailored models for clients to address the data heterogeneity across sites while leveraging shared learning within the federated learning network[15]. Some PFL methods, like pFedBayes[26], FedPop[27], and Self-Aware PFL[28], use probabilistic techniques to mitigate the effects of high data heterogeneity. Other methods, such as FedAP, use batch normalization layers to enhance performance. Detailed information on PFL algorithms can be found in supplement S3.

3 Privacy-Preserving Federated Learning (PPFL)

Ensuring secure processing of protected and identifiable information is crucial in the medical field, where governing regulations strictly prohibit sharing patient data to prevent privacy breaches. Federated learning addresses this by keeping data localized at each site. However, privacy risks persist, as gradient updates exchanged between clients and the server can inadvertently reveal information about training data, leading to privacy leaks[1]. In this section, we present several topics related to PPFL, as depicted in Figure 4 and Table 2. Additional PPFL methods are discussed in detail in supplement S4.

3.1 Differential Privacy

One of the most popular methods for PPFL is differential privacy, which introduces noise into the gradients to prevent private information leakage (Figure 4A)[8]. It provides mathematical guarantees of privacy preservation but potentially at the cost of model accuracy and convergence[10]. Noising before aggregation federated learning (nbAFL), proposed by Wei *et al.,* ensures differential privacy by adding artificial noise to the model parameters on the client side before aggregation, reducing the risk of privacy breaches[29]. To optimize the trade-off between privacy and model performance, nbAFL employs a K-random scheduling technique, where K clients are randomly selected for each aggregation round, making it harder for attackers to extract useful information from the updates. The optimal value of K must be carefully determined to balance privacy and model convergence, a concept known as privacy budget allocation.

3.2 Homomorphic Encryption

As shown in Figure 4B, homomorphic encryption allows mathematical operations to be performed directly on encrypted data, producing encrypted results that, when decrypted, match the results as if the operations had been applied to the original plaintext data[30,31]. This enables secure data sharing with third parties for processing, without exposing the underlying plaintext data. Somewhat homomorphic encryption is a sub-type of homomorphic encryption that permits a limited number of arithmetic operations and is generally more efficient[32]. Somewhat homomorphically encrypted federated learning was used to train models for brain tumor segmentation from MRIs and predict biomarkers from histopathology slides in colorectal cancer[33]. These models achieved performance comparable to standard federated learning models while providing additional privacy guarantees, demonstrating that encryption does not necessarily compromise model accuracy[33]. Notably, these methods encrypted only the vulnerable parts of the federated learning pipeline, resulting in less than a 5% increase in training time and computational cost.

4 Uncertainty Quantification in Federated Learning

Uncertainty quantification in deep learning refers to measuring how confident a model is in its predictions. This is particularly important in medical settings, where both prediction accuracy and reliability are critical for informed decision-making[34]. Uncertainty quantification is vital for fostering trust, reliability, and user acceptance of an AI model[11,34]. It plays a critical role in monitoring model performance post deployment and serves as an early warning system for potential performance degradation, enabling timely human intervention. Additionally, uncertainty quantification can inform decisions on whether to use personalized or global models, assist in detecting out-of-distribution samples, and support active learning during model training. However, in federated learning, uncertainty quantification faces unique challenges due to the non-IID nature of data across participating sites, which often exhibit differing distributions, class imbalances, and other site-specific issues. This section reviews various uncertainty quantification methods specifically designed to address these complexities. Figure 5 and Table 3 provide an overview of uncertainty quantification methods in federated learning, with additional information in supplement S5.

Uncertainty quantification methods can actively enhance federated learning performance in several ways. First, uncertainty-aware client selection can prioritize clients with high-confidence data, improving model convergence. Second, local uncertainty estimates can inform weighting during aggregation, mitigating the impact of low-quality or noisy updates. Third, uncertainty quantification can enable robust deployment by flagging out-of-distribution inputs and guiding fallback mechanisms, such as human review. Finally, in personalized FL, uncertainty estimates can help balance global knowledge with local specialization, improving both generalizability and site-specific performance.

4.1 Uncertainty Quantification using Model Ensembling

Model ensembling is a widely used uncertainty quantification method in federated learning, leveraging its distributed nature by treating multiple clients as an ensemble of models (Figure 5A)[13]. Three key ensembling approaches are ensemble of local models, ensemble of global models, and ensemble based on multiple coordinators[13]. The ensemble of local models prioritizes privacy and simplicity by treating each client's model as an independent member, though it diverges from the collaborative nature of federated learning. The ensemble of global models preserves collaboration but increases computational and communication overhead due to repeated model training with different random seeds. The ensemble based on multiple coordinators improves scalability by distributing clients into subgroups with their coordinators but introduces coordination complexity and the risk of learning fragmentation. Fed-ensemble[35] further expands on these three approaches to address associated limitations. More information about ensembling is provided in supplement S5.

4.2 Uncertainty Quantification using Conformal Prediction

Conformal prediction is a statistical framework that provides a reliable confidence measure for predictions made by ML models (Figure 5B)[36]. Conformal prediction defines a nonconformity measure to assess how different a new example is from previously seen data, generating prediction regions likely to contain the true label or value. Conformal prediction is particularly beneficial in federated learning; however, data heterogeneity among clients violates the assumption of exchangeability, which is fundamental to traditional conformal prediction methods. To address this, Lu *et al.* introduced the concept of partial exchangeability and developed the federated conformal prediction framework. This framework which retains rigorous theoretical guarantees

and demonstrates strong empirical performance across computer vision and medical imaging datasets, making it a practical solution for uncertainty quantification in heterogeneous federated learning environments[37]. More details are provided in supplement S5.

4.3 Uncertainty Quantification using Bayesian Federated Learning

In Bayesian federated learning, shown in Figure 5D, each client learns a posterior probability distribution function (PDF) over its parameters[38,39]. The learned PDF is communicated by the clients to

the server to aggregate the local PDFs and learn a global PDF that can serve all the clients. The posterior PDF can be used for uncertainty quantification in the model's output. Various approximation methods for approximating the posterior PDF, like MC-dropout and Stochastic Weight Averaging Gaussians (SWAG), have also been proposed[13].

4.4 Uncertainty Quantification and Model Output Calibration

Uncertainty quantification methods assess and communicate how confident a model is in its predictions, which is crucial for reliable deployment and decision-making. While these methods directly quantify uncertainty in model outputs, model calibration corrects a model's tendency to be overconfident, particularly due to the Softmax function, thus aligning predicted probabilities with actual performance[11]. By calibrating the Softmax output, a more accurate assessment of the model's confidence is achieved. Luo et al recently introduced the Classifier Calibration with Virtual Representations (CCVR) algorithm, which calibrates a global model to improve performance on non-IID data in heterogeneous settings[40]. The authors found that post-training calibration significantly improves classification accuracy across various federated learning algorithms and datasets[40]. Another recently proposed method, Federated Calibration (FedCal), performs local and global calibration of models[41]. Additional information on calibration methods for federated learning can be found in supplement S5.

While not a standalone uncertainty quantification method, model calibration is an important post-processing technique that aligns predicted confidence scores (e.g., softmax outputs) with empirical accuracy. By correcting for over- or under-confidence, particularly in the presence of non-IID data, calibration enhances the trustworthiness of model predictions. However, unlike methods such as Bayesian inference or conformal prediction, calibration does not directly estimate epistemic or aleatoric uncertainty.

5 Federated Learning in Medical Imaging

With growing research in the field, real-world applications of federated learning in medical imaging are beginning to demonstrate its clinical potential. This section presents federated learning implementation tools, real-world clinical case studies, and the future outlook of federated learning in medical imaging, including challenges and opportunities.

5.1 Planning a Medical Imaging Federated Learning Project

Implementing a federated learning project for medical imaging involves several key steps to ensure success and compliance with privacy standards set by participating institutions and government regulations. Success can be measured by validating a model that outperforms all local models.

The implementation process begins by defining the specific medical imaging problem, such as disease classification, pixel-level segmentation of organs, or the identification of malignant masses in radiological scans. The next step involves selecting the participating institutions, such as hospitals or imaging labs, and determining which site will act as the central server. Site selection is based on ability to collect and pre-process necessary training data needed, train the model, and share updates with the server site over the internet. After identifying collaborators, an appropriate federated learning software framework, such as NVIDIA FLARE, is selected and customized to meet the project's specific needs. This customization may include implementing privacy-preserving techniques and uncertainty quantification algorithms, as well as configuring site-specific software for data loading and resultant storage. The ML model architecture, inputs, and outputs are also determined at this stage before deploying the federated learning software framework at both the server and client sites.

Before model training begins, each site must prepare its data according to standardized

preprocessing and labeling steps agreed upon beforehand. The federated training process commences once the environment is fully set up, with both central server and client configurations in place. During this phase, each client trains the model locally and sends updates

to the central server, which aggregates these updates and redistributes the updated model for further training. This iterative process continues until the model converges. If implemented, uncertainty quantification guides the training process.

After training, the model is evaluated both locally at each site and globally across all sites to assess its performance. Upon achieving satisfactory results, the model is deployed for clinical use or further research, with ongoing monitoring to ensure its effectiveness. The uncertainty quantification data can guide the model selection process for deployment, allow users to monitor the system performance, and trigger a manual review of the model output if necessary. The entire process is thoroughly documented, and reports are prepared to share findings with the research community. Finally, the model is maintained and periodically updated with new data or improved algorithms, ensuring its relevance and accuracy over time, while collaboration between participating sites continues to drive ongoing learning and improvement.

5.2 Federated Learning Implementation Tools

To streamline the federated learning model training, validation, and deployment process, several open-source frameworks and software development kits have been developed. NVIDIA Federated Learning Application Runtime Environment (FLARE) is a well-known open-source software development kit[42]. NVIDIA-FLARE supports various federated learning algorithms, workflows, and privacy-preserving techniques, including differential privacy and homomorphic encryption. OpenFL is another open-source Python library that operates using a static network topology, where clients connect to a central aggregating server via encrypted channels[43]. The workflow is determined by a federation plan agreed upon by all sites before implementation. Originally designed for medical imaging, OpenFL can be adapted for other applications. Fed-BioMed is another open-source framework tailored for biomedical applications of federated learning, offering tools and libraries to manage distributed training, handle heterogeneous data, and ensure privacy and security in biomedical research[44]. Argonne Privacy-Preserving Framework (APPFL) is an open-source Python package that provides tools to implement, test, and validate various aspects of PPFL experiments in simulation settings[45].

5.3 Medical Imaging Federated Learning Studies

- **Federated Tumor Segmentation (FeTS) for Brain Tumors**: FeTS-1.0 was the first large-scale real-world federated learning effort in medical imaging, aiming to identify the optimal weight aggregation approach to train a consensus model across multiple geographically distinct institutions while retaining data locally[46,47]. Presented as a challenge, FeTS evaluated the generalizability of a federated model trained on brain tumor segmentation to unseen, institution-specific data, showcasing the potential of federated learning in real-world medical settings. Building on this, the FeTS-2.0 challenge focused on out-of-sample generalizability for glioblastoma detection and orchestrated the largest real-world medical federated learning deployment in history, with 71 sites across 6 continents. This effort led to the creation of the largest glioblastoma dataset to date, encompassing 6,314 patients. Leveraging this federated learning model, delineation accuracy improved by 33% for surgically targetable tumors and 23% for the full tumor extent compared to a publicly trained model. This challenge demonstrated the potential of federated learning to enhance model performance in healthcare and paved the way for further research. A key insight was that data quality issues often became apparent only after training, as they were revealed by comparing the model's performance against a publicly trained model. It was also observed that simply adding more data does not always lead to significant improvements if data quality is insufficient.

The project employed centralized federated learning using the FedAvg algorithm[14] and was built on the OpenFL framework[43].

- **Federated Learning for Predicting COVID-19 Outcomes**: Dayan *et al.* used federated learning to train a model on COVID-19 data from 20 different institutions worldwide without sharing data[48]. The Electronic Medical Record CXR AI Model (EXAM) was developed to predict the future oxygen needs of patients with COVID-19. The model achieved an average area under the receiver operating characteristic curve (AUC) of over 0.92 in predicting outcomes. The federated model provided a 16% improvement in the AUC and 38% improvement in generalizability over models trained at individual institutions. The study incorporated data from 4 continents and was validated on three independent sites to ensure the robust model performance. The EXAM framework utilized centralized federated learning with the FedAvg algorithm as its aggregation method[14]. The study also implemented differential privacy in their setup, showing that enhanced privacy can be ensured while maintaining performance. This study was one of the largest real-world applications of federated learning, and showcasing its potential to enable large-scale medical AI model training. One limitation highlighted was that the decentralized nature of the data made further analysis beyond the federated training results challenging. Nonetheless, the authors emphasized that the ability of federated learning to deliver high-performing models to institutions with limited data resources is invaluable for advancing ML in clinical applications.

- **ODELIA for Breast Cancer**: The Open Consortium for Decentralized Medical Artificial Intelligence (ODELIA) is an EU-funded research initiative launched on January 1, 2023, aiming to transform healthcare AI through Swarm Learning[49]. Swarm learning enables collaborative model training without sharing patient data, addressing data privacy concerns in medical research. Over five years, ODELIA plans to develop an open-source swarm learning framework and apply it to create an AI algorithm for detecting breast cancer in MRI scans, utilizing a vast, distributed database[49]. This approach is expected to enhance AI development speed, performance, and generalizability, ultimately improving patient care across Europe. By implementing swarm learning, ODELIA seeks to overcome challenges in data collection for healthcare AI, particularly in cancer screening, where ethical and legal obstacles often impede data sharing. The consortium comprises twelve academic and industry partners from across Europe, including institutes from Austria, Germany, Spain, Greece, Netherlands, Belgium, Switzerland, and the University of Cambridge (United Kingdom). This framework will streamline the process of conducting decentralized FL.

- **Real-World Federated Learning in RACOON** Researchers within the German Radiological Cooperative Network (RACOON), a nationwide initiative involving 38 hospitals, conducted a real-world federated learning experiment and published a detailed guide for developing and deploying federated learning infrastructure[50]. This guide outlines key steps, challenges, and current solutions for successfully implementing federated learning in a radiological setting. The authors deployed their infrastructure across 6 hospitals to train a segmentation model for lung pathology detection using a centralized federated learning approach. The authors compared their approach to simpler alternatives, including local model training and ensembling, to justify the added complexity of federated learning. The guide also covers organizational structure, legal requirements, experimental design, and evaluation strategies for setting up federated learning workflows.

- **Real-World Federated Learning for Breast Density Classification** Roth et. al. demonstrated that federated learning can outperform traditional deep learning methods in real-world settings[51]. Their study involved training a model for breast density classification using data

from 7 clinical institutions. Results showed an average improvement of 6.3% over locally trained models and a 45.8% relative gain in generalizability when evaluated on external test data. This work provides empirical evidence of federated learning's effectiveness in improving model generalizability, particularly in settings with limited data.

5.4 Challenges and Opportunities

We presented an overview of federated learning, PPFL, and uncertainty quantification from both technological and algorithmic perspectives. Additionally, we outlined the key steps for implementing a federated learning project and reviewed five case studies demonstrating its application to real-world medical imaging tasks. Despite substantial progress in recent years, federated learning remains in its early stages. Several challenges must be addressed for federated learning to become a standard approach to ML model development in medical imaging. These challenges present opportunities for researchers to further explore and improve the state of federated learning in this field.

1. **Administrative Challenges**: Before implementing a federated learning project, engaging stakeholders from all participating institutions is essential. These stakeholders typically include researchers, the medical imaging team, information technology and cybersecurity experts, contract and agreement management teams, and hospital administrators. Engaging these groups ensures that all aspects of the project, from technical implementation to legal and ethical considerations, are addressed. Ethical approvals from relevant Institutional Review Boards or ethics committees must be obtained to ensure compliance with regulatory standards, particularly concerning patient data privacy and security. Additionally, formal agreements about "weight sharing" between institutions must be established. These agreements should outline whether model weights will be shared in "plain" or "encrypted" formats, addressing concerns related to data security and compliance with privacy laws such as HIPAA or GDPR. These agreements should also specify the responsibilities of each institution, including data governance, data transmission protocols, and contingency plans in case of data breaches. Addressing these issues comprehensively before the federated learning project begins is crucial for ensuring smooth collaboration and maintaining trust among the involved parties.

2. **Requirement for Annotated Datasets**: It is important to recognize that federated learning does not eliminate the need for annotated data. Each participating site must still invest substantial resources in creating and annotating datasets for training local models. The federated learning community should build upon and extend ongoing work in self-supervised learning, active learning, continual learning, and transfer learning to federated environments. One promising area of research involves the use of generative AI models to create diverse, clinically relevant datasets. However, despite their potential, there is currently limited evidence supporting the clinical utility of AI-generated images. This highlights the need for further research to validate their effectiveness in training federated models.

3. **Privacy-Performance Trade-offs**: Another critical challenge in federated learning is the inherent tradeoff between privacy and model performance[29]. Further research is needed to efficiently allocate the privacy budget in a way that enhances privacy protections without compromising model effectiveness. Exploring alternative noise types and noise injection methods offers a promising direction for improving the effectiveness of differential privacy. Additionally, encryption methods, including homomorphic encryption and somewhat homomorphic encryption, must be adapted to federated learning settings to minimize the performance gap between encrypted and unencrypted models. At the same time, communication efficiency between the server and clients remains a key consideration in evaluating the overall effectiveness of federated learning algorithms.

4. **Personalization vs. Generalization in PFL**: PFL offers the advantage of tailoring models to the specific needs of individual clients, which can lead to improved performance on local data. However, this personalization can introduce challenges, including overfitting and reduced generalizability, factors that federated learning typically aims to preserve. Incorporating uncertainty information about model weights calculated during federated runs may help PFL models optimize learning and enhance generalization. Uncertainty quantification-guided PFL has the potential to produce more generalizable, personalized models that effectively capture federated knowledge while performing well on local data. Moreover, conformal prediction-based uncertainty quantification methods, though still in their early stages of development, show promise for further improving the generalizability and personalization of PFL models.

5. **Computational Requirements for uncertainty quantification in federated learning**: Computational efficiency remains an unresolved challenge in uncertainty quantification for federated models, particularly with ensembling and Bayesian approaches. Model ensembling requires training multiple models with different initialization seeds, making it both time- and resource-intensive. Similarly, Bayesian federated learning requires training local models with additional parameters to represent PDFs over model weights, further increasing computational burden. Developing uncertainty quantification methods that are computationally efficient and scalable would be facilitate the widespread adoption of uncertainty quantification in federated learning.

6. **Post-Deployment Performance Monitoring**: Post-deployment performance monitoring using uncertainty quantification methods to identify out-of-distribution and noisy data is a crucial yet relatively unexplored area of research. Uncertainty quantification enables monitoring of model performance, allowing for a human-in-the-loop approach to diagnose and address the causes of model under-performance. This process not only helps resolve immediate issues but also contributes to future model improvement by incorporating the flagged data into subsequent training cycles. As previously discussed, there is considerable opportunity to refine classical uncertainty quantification methods and optimize them for the unique challenges of federated learning.

6 Conclusion

Federated learning has the potential to substantially improve medical imaging workflows in both research and clinical settings. Centralized, decentralized, and personalized federated learning approaches are being developed to tackle a range of healthcare challenges. By enabling collaborative model training across institutions without sharing sensitive patient data, federated learning addresses critical privacy and security concerns while leveraging diverse datasets to enhance model performance and generalizability. Enhanced privacy-preserving techniques , such as differential privacy, homomorphic encryption, and other hybrid approaches, further strengthen data security. Ongoing research incorporating uncertainty quantification in federated learning aims to support the development of more trustworthy AI models. Continued interdisciplinary efforts and technological advancements in this field are expected to further streamline medical imaging workflows, support precision medicine initiatives, and ultimately improve healthcare delivery and patient outcomes worldwide.

References

1. Pati, S., Kumar, S., Varma, A., and Edwards, B. (2024). Privacy preservation for federated learning in healthcare. Patterns *5*. URL: https://www.sciencedirect.com/journal/patterns/vol/5/issue/7. doi:10.1016/j.patter.2024.100974
2. Wiggins, W. F., Magudia, K., Schmidt, T. M. S., O'Connor, S. D., Carr, C. D., Kohli, M. D., and Andriole, K. P. (2021). Imaging AI in Practice: A Demonstration of Future Workflow Using Integration Standards. Radiology: Artificial Intelligence *3*, e210152. URL: https://doi.org/10.1148/ryai.2021210152. PMID: 34350414.
3. Monti, C. B., van Assen, M., Stillman, A. E., Lee, S. J., Hoelzer, P., Fung, G. S. K., Secchi, F., Sardanelli, F., and De Cecco, C. N. (2022). Evaluating the performance of a convolutional neural network algorithm for measuring thoracic aortic diameters in a heterogeneous population. Radiology: Artificial Intelligence *4*, e210196. URL: https://doi.org/10.1148/ryai.210196.
4. Darzidehkalani, E., Ghasemi-rad, M., and van Ooijen, P. V. (2022). Federated Learning in Medical Imaging: Part II: Methods, Challenges, and Considerations. Journal of the American College of Radiology *19*, P755–765. doi:10.1016/j.jacr.2022.03.016.
5. Kaissis, G., Makowski, M., Rü ckert, D., and Braren, R. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence *2*. doi:10.1038/s42256-020-0186-1.
6. Zhang, F., Kreuter, D., Chen, Y., Dittmer, S., and Tull, S. (2024). Recent methodological advances in federated learning for healthcare. Patterns. URL: https://www.cell.com/patterns/fulltext/S2666-3899(24)00131-4. doi:10.1016/j.patter.2024.101006
7. Jere, M. S., Farnan, T., and Koushanfar, F. (2021). A Taxonomy of Attacks on Federated Learning. IEEE Security & Privacy *19*, 20–28. doi:10.1109/MSEC.2020.3039941.
8. Dwork, C. (2006). Differential privacy. In: 33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006). Springer (1–12). doi:10.1007/11787006_1.
9. Gentry, C. A Fully Homomorphic Encryption Scheme. Ph.D. thesis Stanford University (2009). URL: https://crypto.stanford.edu/craig/craig-thesis.pdf.
10. Xu, L., Jiang, C., Qian, Y., Li, J., Zhao, Y., and Ren, Y. (2021). Privacy-Accuracy TradeOff in Differentially-Private Distributed Classification: A Game Theoretical Approach. IEEE Transactions on Big Data. doi:10.1109/TBDATA.2017.2777968.
11. Dera, D., Bouaynaya, N. C., Rasool, G., Shterenberg, R., and Fathallah-Shaykh, H. M. (2021). PremiUm-CNN: Propagating Uncertainty Towards Robust Convolutional Neural Networks. IEEE Transactions on Signal Processing *69*, 4669–4684. doi:10.1109/TSP.2021.3096804.
12. Ahmed, S., Dera, D., Hassan, S. U., Bouaynaya, N., and Rasool, G. (2022). Failure detection in deep neural networks for medical imaging. Frontiers in Medical Technology *4*. URL: https://doi.org/10.3389/fmedt.2022.919046. doi: 10.3389/fmedt.2022.919046
13. Linsner, F., Adilova, L., D ä ubener, S., Kamp, M., and Fischer, A. (2021). Approaches to Uncertainty Quantification in Federated Deep Learning. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer (128–145). URL: https://doi.org/10.1007/978-3-030-93736-2_12.

14. McMahan, B., Moore, E., Ramage, D., Hampson, S., and Arcas, B. A. y. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. In: Singh, A., and Zhu, J., eds. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics vol. 54 of *Proceedings of Machine Learning Research*. PMLR (1273– 1282). URL: https://proceedings.mlr.press/v54/mcmahan17a.html.

15. Lu, W., Wang, J., Chen, Y., Qin, X., Xu, R., Dimitriadis, D., and Qin, T. (2022). Personalized Federated Learning with Adaptive Batchnorm for Healthcare. IEEE Transactions on Big Data (1–1). doi:10.1109/TBDATA.2022.3177197.

16. Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., and Smith, V. (2020). Federated Optimization in Heterogeneous Networks. Proceedings of Machine learning and systems *2*, 429–450. URL: https://proceedings.mlsys.org/paper_files/paper/2020/file/1f5fe83998a09396ebe6477d9475ba0c-Paper.pdf.

17. Li, X., Jiang, M., Zhang, X., Kamp, M., and Dou, Q. (2021). FedBN: Federated Learning on Non-IID Features via Local Batch Normalization. In: International Conference on Learning Representations. URL: https://openreview.net/pdf?id=6YEQUn0QICG.

18. Zhu, Z., Hong, J., and Zhou, J. (2021). Data-Free Knowledge Distillation for Heterogeneous Federated Learning. Proceedings of machine learning research *139*, 12878–12889. URL: https://proceedings.mlr.press/v139/zhu21b.html.

19. Khan, H., Bouaynaya, N. C., and Rasool, G. (2024). Brain-inspired continual learning: Robust feature distillation and re-consolidation for class incremental learning. IEEE Access. URL:https://ieeexplore.ieee.org/abstract/document/10443885. Doi: 10.1109/ACCESS.2024.3369488

20. Yu, Y., Wei, A., Karimireddy, S. P., Ma, Y., and Jordan, M. (2022). TCT: Convexifying Federated Learning using Bootstrapped Neural Tangent Kernels. In: Koyejo, S., Mohamed, S., Agarwal, A., Belgrave, D., Cho, K., and Oh, A., eds. Advances in Neural Information Processing Systems vol. 35. (30882–30897).

21. Huang, W., Ye, M., and Du, B. (2022). Learn from others and be yourself in heterogeneous federated learning. In: 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). (10133–10143). doi:10.1109/CVPR52688.2022.00990.

22. Zhou, T., Zhang, J., and Tsang, D. H. (2023). FedFA: Federated Learning with Feature Anchors to Align Features and Classifiers for Heterogeneous Data. IEEE Transactions on Mobile Computing (1–12). doi:10.1109/TMC.2023.3325366.

23. Warnat-Herresthal, S., Schultze, H., Shastry, K., Manamohan, S., Mukherjee, S., Garg, V., Sarveswara, R., Hä ndler, K., Pickkers, P., Aziz, N. A., Breteler, M., Giamarellos-Bourboulis, E., Kox, M., Becker, M., Cheran, S., Woodacre, M., Goh, E., Schultze, J., and Grundmann, H. (2021). Swarm learning for decentralized and confidential clinical machine learning. Doi: 10.1038/s41586-021-03583-3

24. Kalra, S., Wen, J., Cresswell, J. C., Volkovs, M., and Tizhoosh, H. R. (2023). Decentralized Federated Learning through Proxy Model Sharing. Nature Communications *14*, 2899. doi:10.1038/s41467-023-38569-4.

25. Butt, M., Tariq, N., Ashraf, M., Alsagri, H. S., Moqurrab, S. A., Alhakbani, H. A. A., and Alduraywish, Y. A. (2023). A fog-based privacy-preserving federated learning system for smart healthcare applications. Electronics *12*. URL: https://www.mdpi.com/2079-9292/12/19/4074. doi:10.3390/electronics12194074.

26. Zhang, X., Li, Y., Li, W., Guo, K., and Shao, Y. (2022). Personalized federated learning via variational Bayesian inference. In: Chaudhuri, K., Jegelka, S., Song, L., Szepesvari, C., Niu, G., and Sabato, S., eds. Proceedings of the 39th International Conference on Machine Learning vol. 162 of *Proceedings of Machine Learning Research*. PMLR (26293–26310). URL: https://proceedings.mlr.press/v162/zhang22o.html.

27. Kotelevskii, N., Vono, M., Durmus, A., and Moulines, E. (2022). FedPop: A Bayesian Approach for Personalised Federated Learning. In: Koyejo, S., Mohamed, S., Agarwal, A., Belgrave, D., Cho, K., and Oh, A., eds. Advances in Neural Information Processing Systems vol. 35. Curran Associates, Inc. (8687–8701). URL: https://proceedings.neurips.cc/paper_files/paper/2022/file/395409679270591fd2a70abc694cf5a1-Paper-Conference.pdf.

28. Chen, H., Ding, J., Tramel, E. W., Wu, S., Sahu, A. K., Avestimehr, S., and Zhang, T. (2022). Self-aware personalized federated learning. In: Koyejo, S., Mohamed, S., Agarwal, A., Belgrave, D., Cho, K., and Oh, A., eds. Advances in Neural Information Processing Systems vol. 35. Curran Associates, Inc. (20675–20688). URL: https://proceedings.neurips.cc/paper_files/paper/2022/file/8265d7bb2db42e86637001db2c46619f-Paper-Conference.pdf.

29. Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., Jin, S., Quek, T. Q. S., and Vincent Poor, H. (2020). Federated learning with differential privacy: Algorithms and performance analysis. IEEE Transactions on Information Forensics and Security *15*, 3454–3469. doi:10.1109/TIFS.2020.2988575.

30. Dhiman, S., Nayak, S., Mahato, G. K., Ram, A., and Chakraborty, S. K. (2023). Homomorphic encryption based federated learning for financial data security. In: IEEE International Conference on Innovations in Computer Science and Engineering (I3CS). doi:10.1109/I3CS58314.2023.10127502.

31. Stripelis, D., Saleem, H., Ghai, T., Dhinagar, N. J., Gupta, U., Anastasiou, C., Steeg, G. V., Ravi, S., Naveed, M., Thompson, P. M., and Ambite, J. (2021). Secure neuroimaging analysis using federated learning with homomorphic encryption. In: SPIE Medical Imaging. doi:10.1117/12.2606256.

32. Acar, A., Aksu, H., Uluagac, A. S., and Conti, M. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Comput. Surv. *51*. doi:10.1145/3214303.

33. Truhn, D., Arasteh, S. T., Saldanha, O. L., Müller-Franzes, G., Khader, F., Quirke, P., West, N. P., Gray, R., Hutchins, G. G., James, J. A., Loughrey, M. B., Salto-Tellez, M., Brenner, H., Brobeil, A., Yuan, T., Chang-Claude, J., Hoffmeister, M., Foersch, S., Han, T., Keil, S., Schulze-Hagen, M., Isfort, P., Bruners, P., Kaissis, G., Kuhl, C., Nebelung, S., and Kather, J. N. (2023). Encrypted federated learning for secure decentralized collaboration in cancer image analysis. Medical Image Analysis (103059). doi:https://doi.org/10.1016/j.media.2023.103059.

34. Dera, D., Ahmed, S., Bouaynaya, N., and Rasool, G. (2024). TRustworthy Uncertainty Propagation for Sequential Time-Series Analysis in RNNs. IEEE Transactions on Knowledge & Data Engineering *36*, 882–896. doi:10.1109/TKDE.2023.3288628.

35. Shi, N., Lai, F., Kontar, R. A., and Chowdhury, M. (2023). Fed-ensemble: Ensemble models in federated learning for improved generalization and uncertainty quantification. IEEE Transactions on Automation Science and Engineering (1–0). doi:10.1109/TASE.2023.3269639.

36. Gammerman, A., Vovk, V., and Vapnik, V. (1998). Learning by transduction. In: Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence. UAI'98 San Francisco, CA, USA: Morgan Kaufmann Publishers Inc. ISBN 155860555X (148–155).

37. Lu, C., Yu, Y., Karimireddy, S. P., Jordan, M. I., and Raskar, R. (2023). Federated conformal predictors for distributed uncertainty quantification. In: Proceedings of the 40th International Conference on Machine Learning. ICML'23 JMLR.org.

38. Bhatt, S., Gupta, A., and Rai, P. (2024). Federated Learning with Uncertainty via Distilled Predictive Distributions. In: Yanıkoğ lu, B., and Buntine, W., eds. Proceedings of the 15th Asian Conference on Machine Learning vol. 222 of *Proceedings of Machine Learning Research*. PMLR (153–168).

39. Al-Shedivat, M., Gillenwater, J., Xing, E., and Rostamizadeh, A. (2021). Federated Learning via Posterior Inference: A New Perspective and Practical Algorithms. In: International Conference on Learning Representations. URL: https://openreview.net/forum? id=GFsU8a0sGB.

40. Luo, M., Chen, F., Hu, D., Zhang, Y., Liang, J., and Feng, J. (2021). No Fear of Heterogeneity: Classifier Calibration for Federated Learning with Non-IID Data. Advances in Neural Information Processing Systems *34*, 5972–5984. URL: https://proceedings.neurips.cc/paper_files/paper/2021/file/2f2b265625d76a6704b08093c652fd79-Paper.pdf.

41. Peng, H., Yu, H., Tang, X., and Li, X. (2024). FedCal: Achieving Local and Global Calibration in Federated Learning via Aggregated Parameterized Scaler. In: Salakhutdinov, R., Kolter, Z., Heller, K., Weller, A., Oliver, N., Scarlett, J., and Berkenkamp, F., eds. Forty-first International Conference on Machine Learning vol. 235 of *Proceedings of Machine Learning Research*. PMLR. URL: https://openreview.net/forum?id=XecUTmB9yD.

42. Roth, H., Cheng, Y., Wen, Y., Yang, I., Xu, Z., Hsieh, Y.-T., Kersten, K., Harouni, A., Zhao, C., Lu, K., Zhang, Z., Li, W., Myronenko, A., Yang, D., Yang, S., Rieke, N., Quraini, A., Chen, C., Xu, D., and Feng, A. (2022). NVIDIA FLARE: Federated Learning from Simulation to Real-World. doi:10.48550/arXiv.2210.13291.

43. Patrick Foley and Micah J Sheller and Brandon Edwards and Sarthak Pati and Walter Riviera and Mansi Sharma and Prakash Narayana Moorthy and Shih-han Wang and Jason Martin and Parsa Mirhaji and Prashant Shah and Spyridon Bakas (2022). OpenFL: the open federated learning library. Physics in Medicine & Biology *67*, 214001. doi:10.1088/ 1361-6560/ac97d9.

44. Cremonesi, F., Vesin, M., Cansiz, S., Bouillard, Y., Balelli, I., Innocenti, L., Silva, S., Ayed, S.-S., Taiello, R., Kameni, L., Vidal, R., Orlhac, F., Nioche, C., Lapel, N., Houis, B., Modzelewski, R., Humbert, O., Ö nen, M., and Lorenzi, M. (2023). Fed-BioMed: Open, Transparent and Trusted Federated Learning for Real-world Healthcare Applications. URL: https://arxiv.org/abs/2304.12012. doi: 10.48550/arXiv.2304.12012

45. Ryu, M., Kim, Y., Kim, K., and Madduri, R. K. (2022). APPFL: Open-Source Software Framework for Privacy-Preserving Federated Learning. In: 2022 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). Los Alamitos, CA, USA: IEEE Computer Society (1074–1083). doi:10.1109/IPDPSW55747.2022.00175.

46. Pati, S., Baid, U., Zenk, M., Edwards, B., Sheller, M., Reina, G. A., Foley, P., Gruzdev, A., Martin, J., Albarqouni, S. et al. (2021). The Federated Tumor Segmentation (FeTS) Challenge. arXiv preprint arXiv:2105.05874. URL: https://doi.org/10.48550/arXiv.2105.05874.

47. Pati, S., Baid, U., Edwards, B., Sheller, M., Wang, S.-H., Reina, G. A., Foley, P., Gruzdev, A., Karkada, D., Davatzikos, C. et al. (2022). Federated learning enables big data for rare cancer boundary detection. Nature communications *13*, 7346. URL: https://doi.org/10.1038/s41467-022-33407-5.

48. Dayan, I., Roth, H. R., Zhong, A., Harouni, A., Gentili, A., Abidin, A. Z., Liu, A., Costa, A. B., Wood, B. J., Tsai, C.-S. et al. (2021). Federated learning for predicting clinical outcomes in patients with covid-19. Nature Medicine *27*, 1735–1743. URL: https://www.nature.com/articles/s41591-021-01506-3. doi:10.1038/s41591-021-01506-3.

49. ODELIA (2024). New research project odelia launches to revolutionise artificial intelligence in healthcare using swarm learning. URL: https://odelia.ai/ accessed: 2024-06-17.

50. Bujotzek, M. R., Akü nal, Ü ., Denner, S., Neher, P., Zenk, M., Frodl, E., Jaiswal, A., Kim, M., Krekiehn, N. R., Nickel, M. et al. (2025). Real-world federated learning in radiology: hurdles to overcome and benefits to gain. Journal of the American Medical Informatics Association *32*, 193–205. doi:10.1093/jamia/ocae259.

51. Roth, H. R., Chang, K., Singh, P., Neumark, N., Li, W., Gupta, V., Gupta, S., Qu, L., Ihsani, A., Bizzo, B. C., Wen, Y., Buch, V., Shah, M., Kitamura, F. C., Mendoncca, M. R. F., Lavor, V., Harouni, A. E., Compas, C. B., Tetreault, J., Dogra, P., Cheng, Y., Erdal, S., White, R. D., Hashemian, B., Schultz, T. J., Zhang, M., McCarthy, A., Yun, B. M., Sharaf, E., Hoebel, K. V., Patel, J. B., Chen, B., Ko, S., Leibovitz, E., Pisano, E. D., Coombs, L. P., Xu, D., Dreyer, K. J., Dayan, I., Naidu, R. C., Flores, M. G., Rubin, D. L., and Kalpathy-Cramer, J. (2020). Federated learning for breast density classification: A real-world implementation. In: DART/DCL@MICCAI. URL: https://api.semanticscholar.org/CorpusID:221507926. Doi: 10.1007/978-3-030-60548-3_18

52. Liu, L., Jiang, X., Zheng, F., Chen, H., Qi, G.-J., Huang, H., and Shao, L. (2021). A Bayesian Federated Learning Framework with Online Laplace Approximation. IEEE transactions on pattern analysis and machine intelligence *PP*. URL: https://doi.org/10.1109/TPAMI.2023.3322743.

53. Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., and Zhou, Y. (2019). A Hybrid Approach to Privacy-Preserving Federated Learning. AISec'19 New York, NY, USA: Association for Computing Machinery. ISBN 9781450368339 (1–11). doi:10.1145/3338501.3357370.

54. Xu, R., Baracaldo, N., Zhou, Y., Anwar, A., Kadhe, S., and Ludwig, H. (2022). DeTrust-FL: Privacy-Preserving Federated Learning in Decentralized Trust Setting. In: 2022 IEEE 15th International Conference on Cloud Computing (CLOUD). IEEE (417–426). URL: https://doi.org/10.1109/CLOUD55607.2022.00065.

55. Qi, T., Wu, F., Wu, C., He, L., Huang, Y., and Xie, X. (2023). Differentially Private Knowledge Transfer for Federated Learning. Nature Communications *14*, 3785. doi:10.1038/ s41467-023-38794-x.

56. So, J., Ali, R. E., Gü ler, B., Jiao, J., and Avestimehr, A. S. (2023). Securing secure aggregation: Mitigating multi-round privacy leakage in federated learning. AAAI'23/IAAI'23/EAAI'23 AAAI Press. ISBN 978-1-57735-880-0. doi:10.1609/aaai.v37i8.26177.

57. Wang, T., Yang, Q., Zhu, K., Wang, J., Su, C., and Sato, K. (2024). Lds-fl: Loss differential strategy based federated learning for privacy preserving. IEEE Transactions on Information Forensics and Security *19*, 1015–1030. doi:10.1109/TIFS.2023.3322328.

58. Plassier, V., Makni, M., Rubashevskii, A., Moulines, E., and Panov, M. (2023). Conformal prediction for federated uncertainty quantification under label shift. In: Krause, A., Brunskill, E., Cho, K., Engelhardt, B., Sabato, S., and Scarlett, J., eds. Proceedings of the 40th International Conference on Machine Learning vol. 202 of *Proceedings of Machine Learning Research*. PMLR (27907–27947).

59. Makhija, D., Ghosh, J., and Ho, N. (2023). Privacy preserving bayesian federated learning in heterogeneous settings. arXiv preprint arXiv:2306.07959. URL: https://doi.org/10.48550/arXiv.2306.07959.

60. Sanderson, B. (2018). Uncertainty quantification in multi-model ensembles. Oxford Research Encyclopedia of Climate Science. URL: https://dx.doi.org/10.1093/ACREFORE/9780190228620.013.707. doi:10.1093/ACREFORE/9780190228620.013.707.

61. Krizhevsky, A., and Hinton, G. Cifar-10 (canadian institute for advanced research). Tech. Rep. Canadian Institute for Advanced Research (2009).

62. Krizhevsky, A. (2022). Learning multiple layers of features from tiny images. university of toronto (2012). http://www.cs.toronto.edu/kriz/cifar.html, last accessed *5*, 13.

63. Kuznetsova, A., Rom, H., Alldrin, N., Uijlings, J., Krasin, I., Pont-Tuset, J., Kamali, S., Popov, S., Malloci, M., Kolesnikov, A. et al. (2020). The open images dataset v4. International Journal of Computer Vision (1–26). Doi: 10.1007/s11263-020-01316-z

Tables

Table 1: List and Characteristics of Federated Learning (FL) Algorithms.

Algorithm	Central Server	Local Forget-ting	Summary
FedAvg [14]	✓	X	Train local models across various clients and then average the gradient updates at the central server to update the global mode; first proposed method of FL.
FedProx [16]	✓	X	Excels in heterogeneous settings; generalization of the FedAvg algorithm; allows for partial updates to be sent to the server instead of simply dropping them from a federated round; adds proximal term that prevents any one client from having too much of an impact on the global model.
FedBN [17]	✓	X	Addresses the issue of non-IID data by leveraging batch normalization; follows a similar procedure to Fed-Avg but assumes local models have batch norm layers and excludes their parameters from the averaging step.
FedGen [18]	✓	X	Learns a generator model on the server to ensemble user models' predictions, creating augmented samples that encapsulate consensual knowledge from user models; generate augmented samples that are shared with users to regularize local model training, leading to better accuracy and faster convergence.
FOLA [52]	✓	✓	Bayesian federated learning framework utilizing online Laplace approximation to address local catastrophic forgetting and data heterogeneity; maximizes the posteriors of the server and clients simultaneously to reduce aggregation error and mitigate local forgetting.
Swarm Learning [23]	X	✓	Model parameters are shared via a swarm network, and the model is built independently on private data at the individual sites; only pre-authorized clients are allowed to execute transactions; on-boarding new clients can be done dynamically.
TCT [20]	✓	✓	Train-Convexify-Train: Learn features with an off-the-shelf method (i.e., Fedavg) and then optimize a convexified problem obtained using the model's empirical neural tangent kernel approximation; involves two stages where the first stage learns useful features from the data, and the second stage learns to use these features to generate a well-performing model.
FedAP [15]	✓	X	Learns similarities between clients by calculating distances between batch normalization layer statistics obtained from a pre-trained model; these similarities are used to aggregate client models; each client preserves its batch normalization layers to maintain personalized features; the server aggregates client model parameters weighted by client similarities in a personalized manner to generate a unique final model for each client.
pFedBays [26]	✓	X	Weight uncertainty is introduced in client and server neural networks; to achieve personalization, each client updates its local distribution parameters by balancing its construction error over private data.
FCCL [21]	✓	✓	Federated cross-correlational and continual learning uses unlabeled public data to address heterogeneity across models and non-IID data, enhancing model generalizability; constructs a cross-correlation matrix on model outputs to encourage class invariance and diversity; employs knowledge distillation, utilizing both the updated global model and the trained local model to balance inter-domain and intra-domain knowledge to mitigate local forgetting.
Self-FL [28]	✓	✓	Self-aware personalized FL method that uses intra-client and inter-client uncertainty estimation to balance the training of its local personal model and global model.
Fedpop [27]	✓	X	Each client has a local model composed of fixed population parameters that are shared across clients, as well as random effects that explain heterogeneity in the local data.

FedFA [22]	✓	X	Feature anchors are used to align features and calibrate classifiers across clients simultaneously; this enables client models to be updated in a shared feature space with consistent classifiers during local training.
ProxyFL [24]	✓	X	Clients maintain two models, a private model that is never shared and a publicly shared proxy model that is designed to preserve patient privacy; proxy models allow for efficient information exchange among clients without needing a centralized server; clients can have different model architectures.
FogML [25]	X	X	Fog computing nodes reside on the local area networks of each site; fog nodes can pre-process data and aggregate updates from the locally trained models before transmitting, reducing data traffic over sending raw data.

Note.—IID = independent and identically distributed

Table 2: List of PPFL Algorithms having Differential Privacy (DP), Homomorphic Encryption (HE).

Algorithm	DP	HE	Summary
Hybrid Approach [53]	✓	✓	Combining DP with secure multiparty computation enables this method to reduce the growth of noise injection as the number of parties increases without sacrificing privacy; the trust parameter allows for maintaining a set level of trust.
NbAFL [29]	✓	X	Noising before aggregation FL (NbAFL) Uses K-random scheduling to optimize the privacy and accuracy trade-off by introducing artificial noise into the parameters of each client before aggregation.
DeTrust-FL [54]	X	X	Provides secure aggregation of model updates in a decentralized trust setting; implements a decentralized functional encryption scheme where clients collaboratively generate decryption key fragments based on an agreed participation matrix.
SHEFL [33]	✓	✓	Somewhat homomorphically encrypted FL (SHEFL); only communicating encrypted weights; all model updates are conducted in an encrypted space.
PrivateKT [55]	✓	X	Private knowledge transfer method that uses a small subset of public data to transfer knowledge with local DP guarantee; selects public data points based on informativeness rather than randomly to maximize the knowledge quality.
Multi-RoundSecAgg [56]	✓	X	Provides privacy guarantees over multiple training rounds; develops a structured user section strategy that guarantees the long-term privacy of each use.
LDS-FL [57]	X	X	Maintain the performance of a private model preserved through parameter replacement with multi-user participation to reduce the efficiency of privacy attacks.

*Note DP: differential Privacy, FL: Federated Learning

Table 3 : Uncertainty quantification Methods in federated learning.

Algorithm	CP	Dist Pred	Bayes	Cal	Summary
CCVR[40]	✗	✗	✗	✓	Classifier calibration with Virtual Representation (CCVR) Found a greater bias in representations learned in the deeper layers of a model trained with FL; they show that the classifier contains the greatest bias toward local client data and that classification performance can be greatly improved with post-training classifier calibration
Fed-ensemble[35]	✗	✗	✗	✗	Extends ensembling methods to FL; characterizes uncertainty in predictions by using the variance in the predictions as a measure of knowledge uncertainty.
DP-fedCP[58]	✓	✗	✗	✗	Differentially Private Federated Average Quantile Estimation (DP-fedCP); the method is designed to construct personalized CP sets in an FL scenario.
FCP[37]	✓	✗	✗	✗	Federated CP, a framework for extending CP to FL that addresses the non-IID nature of data in FL.
FedPPD[38]	✗	✓	✗	✗	Framework for FL with uncertainty, where, in every round, each client infers the posterior distribution over its parameters and the posterior predictive distribution (PPD); PPD is sent to the server.
FedBNN[59]	✗	✗	✓	✗	FL framework based on training a customized local Bayesian model for each client.
FedCal[41]	✗	✗	✗	✓	Performs local and global calibration of models. FedCAL uses client-specific parameters for local calibration to effectively correct output misalignment without sacrificing prediction accuracy. Values are then aggregated via weight averaging to minimize global calibration error

Note.—CP: Conformal Prediction, Dist Pred: Distilled Prediction, Bayes: Bayesian, Cal: Calibration

7 Figure Legends

- **Figure 1** -**Organization of the review paper.** The figure outlines the structure of the paper, beginning with an introduction to federated learning (FL) in medical imaging. It progresses through the classification of FL algorithms into centralized, decentralized, and personalized (PFL) categories, followed by discussions on privacy-preserving methods and uncertainty quantification (UQ). The review concludes with applications of FL in medical imaging, including real-world use cases, challenges, and opportunities. This visual representation highlights the interconnected topics covered in the review and provides readers with a clear roadmap for understanding the paper's flow and content.
- **Figure 2** - An overview of Federated Learning (FL),Privacy Preserving Federated Learning (PPFL), and uncertainty quantification (UQ) is presented. Combining FL with strong privacy preservation and uncertainty quantification methods can help the medical imaging community develop large-scale Mult institutional AI models that are truly generalizable, robust, and trustworthy.
- **Figure 3** - An overview of federated learning (FL) algorithm types is presented. (A) In centralized FL, sites train a local model and pass the learned information to a central server to generate the global model, the global model is then passed to the local sites for further training. (B) Decentralized FL removes the need for a central server allowing for direct communication between sites. (C) Personalized FL leverages a central server while making a specific model for each site. Having a personalized model at each site is ideal in FL deployments with high data heterogeneity.
- **Figure 4** - A summary of privacy-preserving FL (PPFL) methods is presented. (A) Differential Privacy (DP) involves the addition of artificial noise into other gradient information before it is communicated, hindering the ability of an attacker to extract useful information. (B) Homomorphic Encryption (HE) allows for mathematical operations to be performed on encrypted cyphertexts, and then once decrypted the results are as if the math was performed on plaintext. HE is useful in situations where the central server cannot be trusted. (C) Various other methods of PPFL include hybrid approaches of DP and HE, knowledge transfer, secure aggregation framework with multi-round privacy, loss differential strategies, and decentralized trust. More information about these other PPFL approaches is described in supplement S4.
- **Figure 5** - A summary of uncertainty quantification (UQ) methods in Federated Learning (FL is presented. (A) Model ensembling refers to the process of training various models; the final result is the average of their predictions. (B) Conformal Prediction (CP) is a method of UQ that provides a set of possible predictions, where the more uncertain the model is the more possible predictions it will provide. (C) Model calibration is a post-processing reliability enhancement technique that adjusts predicted confidence scores to better reflect true correctness likelihood. While not a direct uncertainty quantification method, it improves the trustworthiness of model outputs by mitigating overconfidence, especially in misclassified predictions, and aligns predicted probabilities with actual observed frequencies. (D) Bayesian FL is another method of UQ that tracks the variance of the model during training and at inference time. The variance will go up as the model becomes more uncertain providing a measure of model uncertainty.

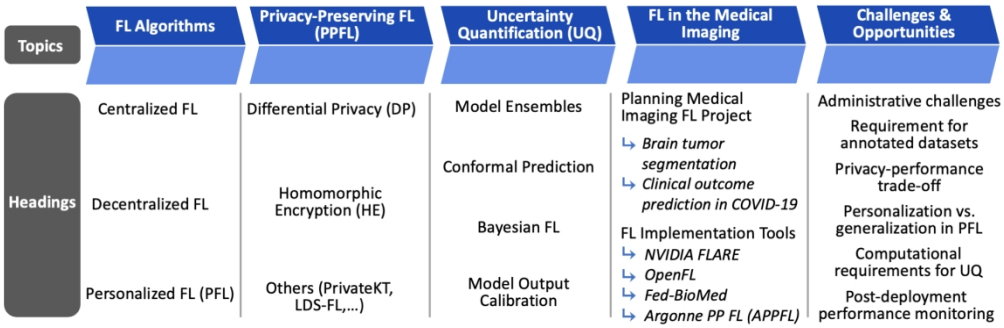
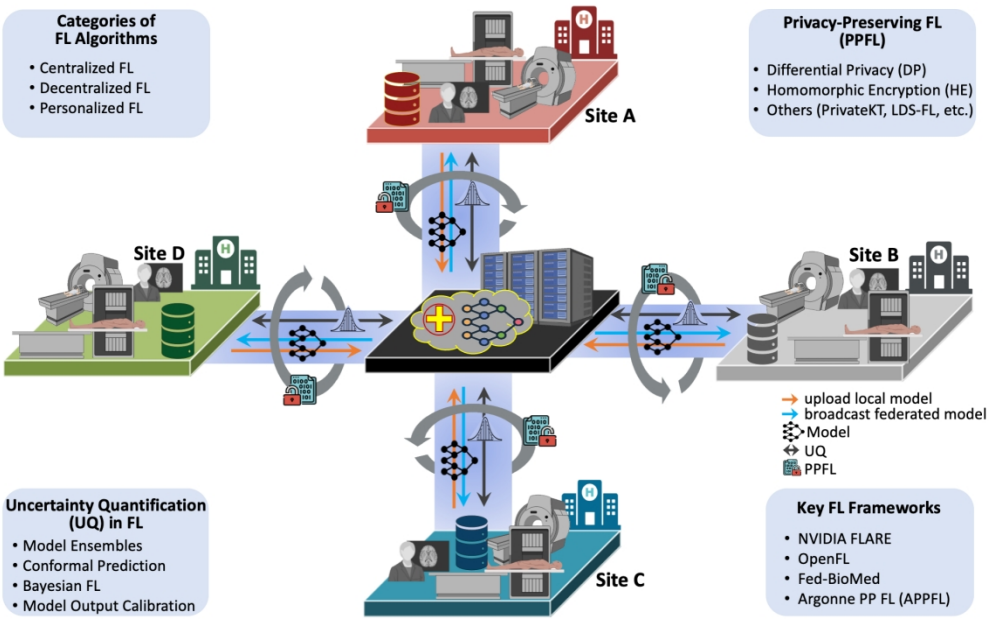


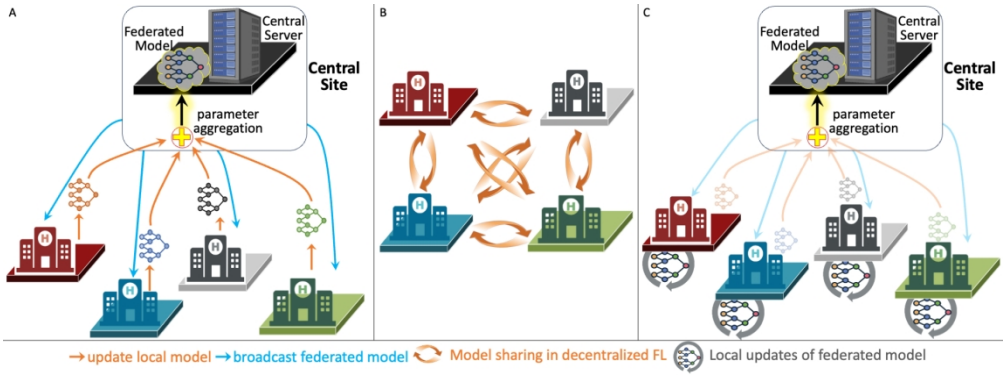
Figure 1 -Organization of the review paper. The figure outlines the structure of the paper, beginning with an introduction to federated learning (FL) in medical imaging. It progresses through the classification of FL algorithms into centralized, decentralized, and personalized (PFL) categories, followed by discussions on privacy-preserving methods and uncertainty quantification (UQ). The review concludes with applications of FL in medical imaging, including real-world use cases, challenges, and opportunities. This visual representation highlights the interconnected topics covered in the review and provides readers with a clear roadmap for understanding the paper's flow and content.

528x170mm (96 x 96 DPI)



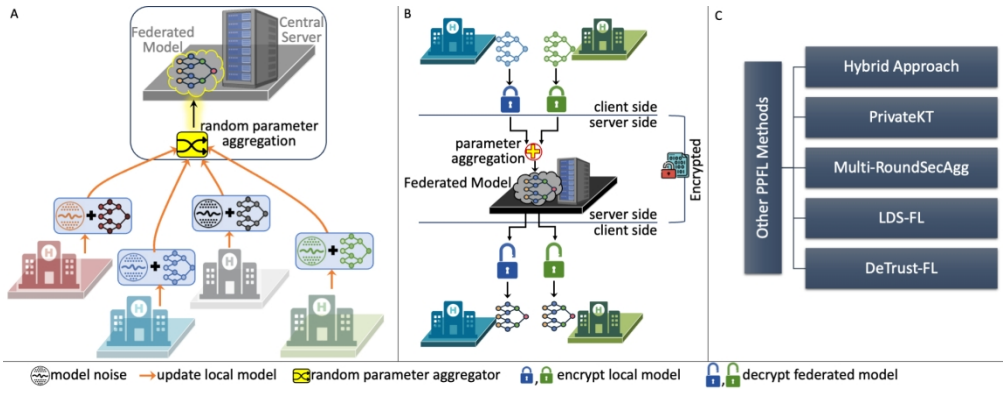
• Figure 2 - An overview of FL, PPFL, and UQ is presented. Combining FL with strong privacy preservation and uncertainty quantification methods can help the medical imaging community develop large-scale Mult institutional AI models that are truly generalizable, robust, and trustworthy.

465x287mm (109 x 109 DPI)



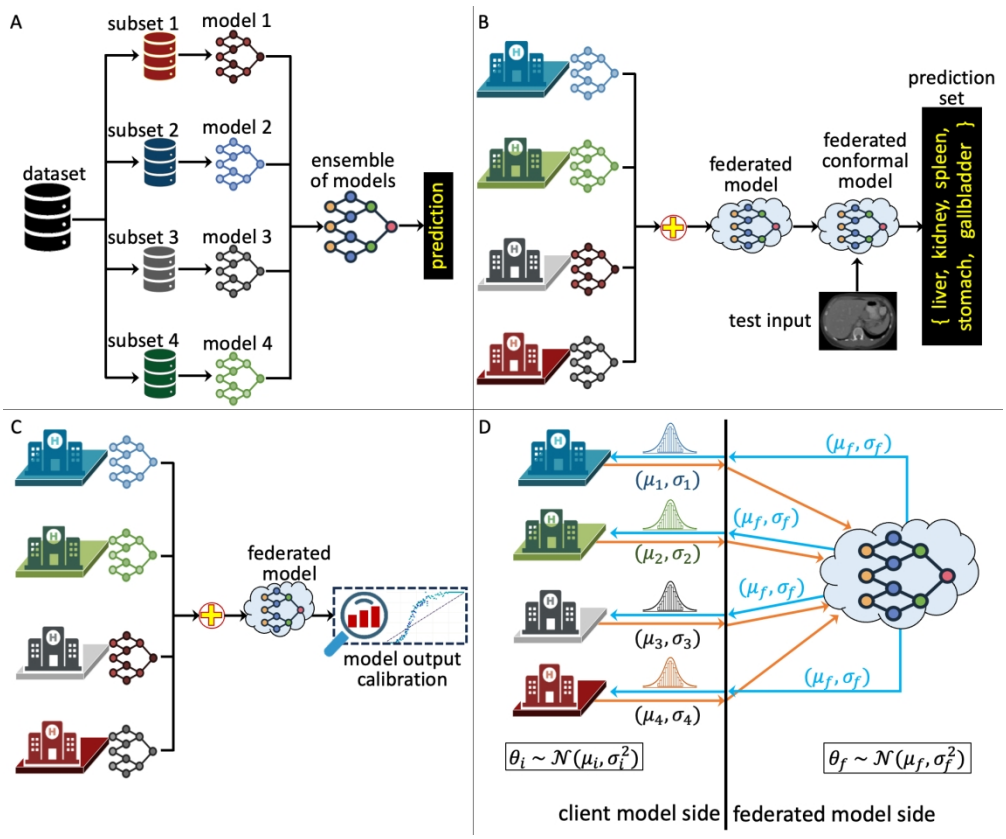
• Figure 3 - An overview of FL algorithm types is presented. (A) In centralized FL, sites train a local model and pass the learned information to a central server to generate the global model, the global model is then passed to the local sites for further training. (B) Decentralized FL removes the need for a central server allowing for direct communication between sites. (C) Personalized FL leverages a central server while making a specific model for each site. Having a personalized model at each site is ideal in FL deployments with high data heterogeneity.

488x181mm (104 x 104 DPI)



• Figure 4 - A summary of privacy-preserving FL (PPFL) methods is presented. (A) Differential Privacy (DP) works by adding artificial noise into other gradient information before it is communicated, this hinders the ability of an attacker to extract useful information. (B) Homomorphic Encryption (HE) allows for mathematical operations to be performed on encrypted cyphertexts, and then once decrypted the results are as if the math was performed on plaintext. HE is useful in situations where the central server cannot be trusted. (C) Various other methods of PPFL include hybrid approaches of DP and HE, knowledge transfer, secure aggregation framework with multi-round privacy, loss differential strategies, and decentralized trust. More information about these other PPFL approaches is described in supplement S4.

457x175mm (111 x 111 DPI)



• Figure 5 - A summary of UQ methods in FL is presented. (A) Model ensembling is where various models are trained and the final result is the average of their predictions. (B) Conformal Prediction (CP) is a method of UQ that provides a set of possible predictions, where the more uncertain the model is the more possible predictions it will provide. (C) Model calibration is a post-processing UQ method that serves to correct the issue of overconfidence in model prediction particularly when the model makes an incorrect prediction. This allows for more trustworthy confidence measures in the model's predictions. (D) Bayesian FL is another method of UQ that tracks the variance of the model during training and at inference time. The variance will go up as the model becomes more uncertain providing a measure of model uncertainty.

300x248mm (169 x 169 DPI)