Review Article

Healthc Inform Res. 2024 January;30(1):3-15.
https://doi.org/10.4258/hir.2024.30.1.3
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Survey of Medical Applications of Federated Learning

Geunho Choi[1], Won Chul Cha[1,2], Se Uk Lee[2], Soo-Yong Shin[1]

[1]Department of Digital Health, SAIHST, Sungkyunkwan University, Seoul, Korea
[2]Department of Emergency Medicine, Samsung Medical Center, Sungkyunkwan University School of Medicine, Seoul, Korea

Objectives: Medical artificial intelligence (AI) has recently attracted considerable attention. However, training medical AI models is challenging due to privacy-protection regulations. Among the proposed solutions, federated learning (FL) stands out. FL involves transmitting only model parameters without sharing the original data, making it particularly suitable for the medical field, where data privacy is paramount. This study reviews the application of FL in the medical domain. **Methods:** We conducted a literature search using the keywords "federated learning" in combination with "medical," "healthcare," or "clinical" on Google Scholar and PubMed. After reviewing titles and abstracts, 58 papers were selected for analysis. These FL studies were categorized based on the types of data used, the target disease, the use of open datasets, the local model of FL, and the neural network model. We also examined issues related to heterogeneity and security. **Results:** In the investigated FL studies, the most commonly used data type was image data, and the most studied target diseases were cancer and COVID-19. The majority of studies utilized open datasets. Furthermore, 72% of the FL articles addressed heterogeneity issues, while 50% discussed security concerns. **Conclusions:** FL in the medical domain appears to be in its early stages, with most research using open data and focusing on specific data types and diseases for performance verification purposes. Nonetheless, medical FL research is anticipated to be increasingly applied and to become a vital component of multi-institutional research.

Keywords: Machine Learning, Deep Learning, Distributed Systems, Privacy, Data Security

I. Introduction

Artificial intelligence (AI) has recently emerged as a promising tool in medical research and applications [1,2]. The performance of AI, particularly in machine learning and deep learning, improves and stabilizes with access to large datasets. Consequently, researchers have been motivated to amass substantial amounts of data, often referred to as big data. However, traditional AI models necessitate centralized data repositories, which pose significant concerns for the protection of sensitive medical information. In response, privacy-protection regulations such as the General Data Protection Regulation (GDPR) in the European Union [3], the Health Insurance Portability and Accountability Act (HIPAA) in the United States [4], and the Personal Information Protection Act in Korea [5] have been enacted to secure personal data, including medical and healthcare records. As a result, medical AI development must adhere to these regulations, requiring researchers to implement appropriate privacy-preserving

Submitted: October 5, 2023
Revised: 1st, January 5, 2024; 2nd, January 23, 2024
Accepted: January 24, 2024

Corresponding Author
Soo-Yong Shin
Department of Digital Health, SAIHST, Sungkyunkwan University, 81, Irwon-ro, Gangnam-gu, Seoul 06351, Korea. Tel: +82-2-3410-1449, E-mail: sy.shin@skku.edu (https://orcid.org/0000-0002-2410-6120)

methods.

Several methods for protecting privacy have been proposed, including de-identification techniques such as differential privacy [6,7], the generation of synthetic data [8-10], homomorphic encryption [11-13], and federated learning (FL) [14]. Our focus is on the privacy-preserving attributes of FL. The process of FL is as follows: each client independently trains a model on their local data, ensuring that individual data remains secure and is not exposed externally. The clients then transmit their model parameters to a central server. This server aggregates the parameters received from all clients to create a global model. Once the central server distributes the global model back to the clients, they perform additional local training using this model. The updated parameters are then sent back to the central server, which uses them to develop the subsequent iteration of the global model.

The fact that FL utilizes local client resources without the need for centralized resources and data has attracted interest as a privacy-preserving alternative. This is particularly relevant for hospitals, which often hold clinical data but are hesitant to share or expose the data due to privacy concerns. Originally, FL was proposed to leverage the unused resources of handheld devices. The primary distinction between FL in institutional settings, such as hospitals (referred to as on-site FL), and FL that taps into the resources of handheld devices (known as on-device FL), lies in the number of clients. On-device FL typically involves a significantly larger number of clients than on-site FL, where the clients often form a data silo and number in the single to double digits. Since medical data are housed within a hospital, FL involving medical data typically takes the form of on-site FL.

Review papers on FL in the medical domain have been published [15-19]; however, these studies have only introduced a limited number of examples of medical FL research. Our study differs from existing FL reviews by concentrating on specific instances of medical FL research. Additionally, we have organized the selected FL papers according to (1) the types of data utilized, (2) the targeted disease, (3) the use of an open dataset, (4) the local model of FL, and (5) the neural network model employed. This study categorizes and analyzes current medical FL research to provide insights into areas that have been well-explored and those that remain underexplored.

II. Methods

A literature search was conducted using the keywords "federated learning" combined with "medical," "healthcare," or "clinical" on Google Scholar and PubMed. This search took place in September 2022 and was not restricted by publication year. Initially, the search yielded 129,000 papers on Google Scholar and 173 on PubMed. We arbitrarily chose to review the first 400 articles listed on Google Scholar, which is more than double the number of articles found on PubMed. From this initial set of 400 papers, we carefully selected 58 papers by applying specific exclusion criteria. These criteria excluded papers that only presented methodology without using medical data, papers that were inaccessible or could not be downloaded, and studies that were duplicates.

To extract insights from the papers we reviewed, we organized the studies according to several criteria: (1) the types of data utilized, including images, free text, signals, and laboratory data; (2) the disease of interest; (3) the employment of open datasets; (4) the type of local model applied in FL, distinguishing between machine learning and neural network models; and (5) the implementation of neural network models within the context of FL.

According to previous literature reviews on FL [15-17,20], heterogeneity and security concerns were frequently discussed. Therefore, we explored the extent to which studies addressed these issues. We also examined whether any of the papers proposed countermeasures to mitigate these concerns.

III. Results

According to our literature survey, the first article [14] on FL was published in 2016 and the first article [21] on the medical applications of FL was published in 2019. In 2019, three articles were published, followed by 11 in 2020, 29 in 2021, and 15 in 2022. This trend demonstrates a growing interest in FL research within the medical field. Table 1 provides a summary of these studies, categorizing them by their target diseases and the types of data utilized [21-78].

1. Data Types

The most frequently utilized data type in the reviewed studies was image data, represented in 36 studies. This was followed by laboratory data in nine studies, free text and signals, each in six studies, mobile health data in a single study, and genomic data also in one study. Among the 58 studies reviewed, only one combined two types of data—image and laboratory data [35].

Among the 36 studies that used image data, the distribution was as follows: 24 studies used radiology images, six

Table 1. Summary of data types, target diseases, and key findings of federated learning (FL) medical-domain research

Reference	Data type	Target disease	Key finding
[21-27]	Image	Cancer	FL with radiology images was used in cancer research.
[28-33]	Image	Cancer	FL was used to study pathological images of cancers.
[34]	Image	Thyroid nodule	Ultrasound image analysis using FL was utilized to predict whether thyroid nodules were benign or malignant.
[35]	Image, Lab data	COVID-19	A model was built using FL with data from over 20 institutions to predict the future oxygen requirements of symptomatic COVID-19 patients.
[36-43]	Image	COVID-19	COVID-19 detection models using FL were built.
[44-46]	Image	-	Radiology image reconstruction models using FL were built.
[47]	Image	-	FL was used to build a model for breast density classification using breast images from seven multinational clinical institutions.
[48]	Image	Diabetic retinopathy	A system that utilized FL with differentially private stochastic gradient descent, in combination with secure aggregation, was proposed.
[21,22,27,49-51]	Image	Nervous system diseases, -	FL was used in studies of brain tumors, autism spectrum disorders, brain age prediction, and multiple sclerosis. These studies showed that FL can be applied to research using nervous system radiology images.
[52]	Image	Cardiovascular disease	FL was used to diagnose cardiovascular disease using cardiac MRI data.
[53,54]	Image	Skin diseases	Models for detecting skin diseases were built using FL.
[55]	Image	-	A method for federated semi-supervised learning of surgical phases was presented.
[56]	Image	Melanoma	FL was used in a study on melanoma detection using skin images.
[57,58]	Free text	Psychiatric disease	The potential of FL for clinical psychiatry was highlighted.
[59-61]	Free text	Vaccine adverse events, -	Named entity recognition, entity recognition, and relation extraction tasks were performed with FL. It was demonstrated that natural language processing models can be built using FL.
[62]	Free text	-	A personalized clinical decision support system based on FL to assist healthcare professionals in medical diagnosis was proposed.
[63-65]	Signal	Major depressive disorder, arrhythmia, stress	FL was used to study major depressive disorder, arrhythmia, and stress using heart-activity data.
[66]	Signal	Parkinson's disease	The first federated transfer learning framework for wearable healthcare was proposed.
[67,68]	Signal	-	An FL-based health-monitoring system was proposed.
[69]	Lab data	Lung cancer, COPD	FL models were trained to predict the risks of diseases associated with tobacco and radon using data from electronic health records.
[70]	Lab data	Adverse drug reaction	FL was used to predict adverse drug reactions using electronic health data.
[71-73]	Lab data	COVID-19	The relationship between COVID-19, mortality, and diseases (acute kidney injury, and cancer) was studied using FL.
[73-76]	Lab data	Mortality	A model to predict mortality in intensive care units using FL was built.
[77]	Other	Depression	An FL-based method for detecting depression was proposed.
[78]	Other	Heart failure	Based on the patient's genomic data, the risk of specific heart failure or cancer diseases was predicted.

The key findings are modified summary sentences from the references. "-" in the target disease column indicates no target disease. MRI, magnetic resonance imaging; COPD, chronic obstructive pulmonary disease; Lab data, laboratory data.

studies utilized pathology images, three studies focused on skin images, two studies examined ultrasound images, and two studies involved other types of images, including fundus and surgical images. Notably, one study utilized two types of images: radiology and ultrasound [43]. Of the 24 studies involving radiology images, chest radiology images were the most common, with 10 studies [26,35-43] examining chest X-rays and chest computed tomography (CT) scans. Six studies investigated nervous system radiology images, delving into topics such as autism spectrum disorder using functional magnetic resonance imaging (MRI) [49], brain age prediction [50], brain tumor segmentation [21], multiple sclerosis lesion segmentation [51], brain tumor MRI [22], and glioblastoma using multiparametric MRI [27]. Additionally, three studies were dedicated to radiology image reconstruction, with two focusing on MRI [44,45] and one on CT [46]. The remaining five studies explored a variety of radiology images, including mammography [24,47], prostate MRI [23], cardiac MRI [52], and pancreatic CT [25]. Pathology images were the focus of six studies, which included applications of differential privacy to pathological images [28], use of the open datasets Camelyon16 and Camelyon17 [29], analysis of gigapixel whole-slide images [30], brain pathology segmentation [31], colorectal cancer data analysis [32], and examination of tumor-infiltrating lymphocytes in whole-slide images [33]. Three studies focused on skin images, tackling issues such as skin disease detection using the Dermatology Atlas dataset [53,54] and melanoma detection with the dermoscopic skin lesion image dataset [56]. Two studies involved ultrasound images [34,43], and the final two studies used other image types, specifically fundus [48] and surgical images [55].

The use of free text in studies was primarily associated with natural language processing, as evidenced by six studies. These investigations encompassed a range of applications: a violence risk assessment [57], benchmarking bidirectional encoder representations from transformers (BERT) models [58], a named entity recognition task [59], detecting adverse events related to vaccines [60], developing a medical relation extraction model [61], and creating a deep learning-based personalized clinical decision support system [62].

Signal data primarily consisted of time-series data obtained from medical devices, and six case studies used this type of data. Research on FL using signal data has largely concentrated on disease research involving heart-activity data or the development of health-monitoring systems. The identified objectives for FL research using signal data included predicting the severity of major depressive disorder based on heart rate variability [63], detecting arrhythmias through electrocardiography [64], automatically detecting stress using heart-activity signals [65], implementing wearable healthcare solutions [66], monitoring health at home [67], and developing health-monitoring systems that employ wearable sensing devices [68].

Furthermore, nine studies utilized laboratory data. These studies focused on predicting various outcomes, including disease risks from electronic health record systems [69], adverse drug reactions [70], mortality within 7 days of hospitalization in COVID-19 patients [71], acute kidney injury within three and seven days of admission [72], patient mortality and length of stay in the intensive care unit [74], and intensive care unit mortality using the MIMIC-III benchmark database [76]. Additionally, they involved evaluating FL with existing datasets [73] and assessing the performance of FL on two typical electronic health record machine learning tasks [75].

Data that did not fall into the categories of image, free text, signals, or laboratory data were categorized as "other." Two studies that belonged to the "other" category were depression detection from mobile data [77] and prediction of disease from genomic data [78].

2. Target Diseases

The most common target disease was cancer (17 studies, one of which [34] involved thyroid nodules) [21-34,56,69,73]. The second most common target disease was COVID-19 (12 studies) due to the recent worldwide COVID-19 pandemic [35-43,71-73]. The remaining 29 studies did not include specific target diseases.

3. Use of Open Datasets

We evaluated whether the data utilized in the studies were open or private [21-78] (Table 2), as the source of the data is important in medical research. Overall, 37 studies used open data, 11 used private data, and 10 used a combination. As can be seen, open datasets were primarily used.

4. Local Models Used in FL

We investigated whether the local models used for FL research were deep or machine learning [21-78] (Table 2). In total, 53 used neural networks as the local models, one used machine learning as the local model, and four used a combination of both. Thus, the majority of the investigated FL studies chose neural networks as the local models.

Table 2. Summary of federated learning studies: the usage of open datasets and the type of local model used for federated learning

Reference	Open data vs. private data	Local model
[21,22,25,26,28,29,32,33,37-41,43,45,46,48-50, 52-54,56,58-62,64,67,68,74-77]	Open data	Neural network
[34-36,47,57,63,65,69]	Private data	Neural network
[23,24,27,30,31,42,44,51,55,66]	Open data + Private data	Neural network
[73]	Open data	Neural network, Machine learning
[70-72]	Private data	Neural network, Machine learning
[78]	Open data	Machine learning

Table 3. Neural network models used in federated learning

Reference	Model	Optimization method
[21,23-25,27,29,33,34,37,40,42, 43,46,47,52-55]	CNN	Adam
[22,26,44,51]	CNN (U-Net)	Adam, SGD
[28]	Memory-based exchangeable model [79]	Adam
[36,39,48,50,56,63,64,66]	CNN	SGD, Mini-batch SGD
[38,41,45]	CNN	RMSProp, Not described, Adamax
[30,59]	Combination of CNN and others	Adam
[35]	Deep & cross network [80]	Adam
[32]	GAN	Adam
[58]	BERT	Adam
[61]	BERT	Cross entropy
[62]	RNN	Not described
[60,68]	BiLSTM	Mini-batch SGD, SGD
[31,67,74]	Autoencoder	SGD, Adam
[49,71,72]	MLP (three hidden layers)	Adam
[65,69,75]	Shallow neural network (two hidden layers)	Adam, SGD, Not described
[57,70,73]	Shallow neural network (one hidden layer)	Mini-batch gradient descent, SGD, Adam
[76]	RNN, LSTM, GRU, and CNN	Adam
[77]	Later fusion model	RMSProp

CNN: convolutional neural network, SGD: stochastic gradient descent, GAN: generative adversarial networks, BERT: bidirectional encoder representations from transformers, RNN: recurrent neural network, BiLSTM: bidirectional long short-term memory, MLP: multilayer perceptron, GRU: gated recurrent unit.

5. Utilization of Neural Network Models in FL

Among the studies we evaluated, neural network algorithms were employed in most cases [21-77,79,80], with only one study being the exception [78] (Table 3). A significant number of these studies, 35 to be exact, utilized convolutional neural networks (CNNs) as their primary model [81]. CNNs were predominantly used in research involving image and signal data [63,64,66]. In contrast, studies that focused on free text primarily implemented recurrent neural networks, including long short-term memory networks [82], and some incorporated the more recent BERT [83]. For laboratory test data, which typically has lower complexity compared to image or signal data, simpler neural network architectures were favored, such as shallow networks with one or two hidden layers, or multilayer perceptron models

Regarding optimization methods, the Adam optimizer [84] emerged as the most commonly used, being adopted in 35 of the 57 studies. The most widely employed method was stochastic gradient descent (SGD) [85], with mini-batch SGD being the second most utilized, serving as the optimization technique in 13 studies. Notably, two studies did not explicitly specify the optimization method employed [38,62].

6. Commonly Mentioned Issues

Although many algorithms employed in FL assume independent and identically distributed (IID) data, real-world data often deviate from this assumption, being non-IID. FedAvg [14], a prominent algorithm in FL, demonstrates slow convergence and suboptimal accuracy when dealing with non-IID data. Since the data characteristics vary across clients, the performance of the global model suffers. This problem is known as the heterogeneity issue.

FL offers advantages in terms of privacy; however, it is still susceptible to security attacks. The most concerning attack in the medical field is the inference attack, which aims to deduce sensitive information from the learning data. Research on inference attacks in FL includes a study on the use of generative adversarial networks for such attacks [86], an examination of inference attacks in vertical FL [87], an analysis of membership inference attacks that could lead to privacy breaches [88], and an investigation into source inference attacks that can extract more information than traditional inference methods [89]. A poisoning attack compromises the performance of FL by reducing the accuracy of the global model through malicious updates. Various studies have explored poisoning attacks, including those on model poisoning that aim to cause misclassification [90,91], research on data poisoning where malicious participants submit updates from incorrectly labeled data [92], a study on FL poisoning attacks utilizing generative adversarial networks [93], and an examination of FL's vulnerability to Sybil-based poisoning attacks [94]. Collectively, these security threats [95] to FL are referred to as "security issues."

Among the 58 articles, 42 (72%) mentioned non-IID data or heterogeneity issues, and 29 (50%) noted security issues. In addition, 22 articles (37%) pointed out both issues, whereas 10 articles (17%) mentioned neither issue.

1) Countermeasures against the heterogeneity issue

To address the issue of heterogeneity, researchers have proposed algorithms that perform well with non-IID data. Two notable algorithms are as follows: Li et al. [96] introduced FedProx, which enhances stability in heterogeneous environments by incorporating a proximal term. Karimireddy et al. [97] identified that data heterogeneity can cause client drift, leading to a decline in FL performance. To counteract this, they developed the SCAFFOLD algorithm, which corrects client drift and has been shown to be at least as efficient as SGD. Li et al. [98] evaluated the accuracy and communication efficiency of several leading FL algorithms, including FedAvg, FedProx, SCAFFOLD, and FedNova, across a range of non-IID scenarios. Their experiments indicated that no single algorithm consistently outperformed the others under the various non-IID conditions. This issue of heterogeneity has also been noted in the widely studied context of handheld device-based FL [96]. However, FL in hospitals (onsite FL) involves a significantly smaller number of clients—ranging from single to double digits—which can make the model more susceptible to bias and exacerbate heterogeneity issues. Consequently, these issues are more pronounced in hospital FL, necessitating the development of specific countermeasures. Despite extensive research aimed at enhancing the performance of global models in non-IID situations, an approach that is both cost-effective and universally effective in all non-IID contexts has yet to be discovered [98].

2) Countermeasures against security issues

In medical FL, the use of patient data necessitates stringent security and privacy protections. To protect against security threats, measures such as differential privacy and homomorphic encryption can be implemented. Our review of FL studies revealed that 11 papers [21,24,28,30,35,48,49,58,60,73,78] employed differential privacy as a security measure, while four papers [36,48,66,67] utilized homomorphic encryption. Differential privacy emerged as the most commonly adopted security measure. It can be easily applied by adding Gaussian noise [6,24,30,48]. In contrast, homomorphic encryption is more challenging to implement than differential privacy and incurs additional computational costs [11,99,100]. Consequently, differential privacy has been more frequently adopted than homomorphic encryption in medical FL research.

IV. Discussion

In this survey, studies within the medical domain that utilized FL were reviewed. The selected FL papers were categorized based on the following criteria: (1) the types of data used, (2) the target disease, (3) the use of an open dataset, (4) the local model of FL, and (5) the employment of neural network models in FL.

Most studies used image data, while relatively few studies utilized free text, signal, and laboratory data. In the broader context of medical research, free text, signals, and laboratory data are frequently used; however, these data types appear to be underrepresented in the field of medical FL research. Cancer and COVID-19 emerged as the most frequently studied diseases in medical FL. In contrast, there have been relatively few FL studies focusing on cardiovascular diseases [101,102] and neurological disorders [103,104], such as Alzheimer's disease, epilepsy, Parkinson's disease, and schizophrenia, despite the active research efforts in these areas. Upon examining the data types and target diseases within medical FL research, a pattern of high research frequency for certain data types and diseases becomes evident. It is noteworthy that among the data types commonly used in medical research and the diseases that are the focus of active study, there are instances where FL is less frequently applied. This observation suggests that FL has the potential to be leveraged across a diverse range of data types and for the study of various diseases.

We also investigated whether the datasets used were open or private. Most studies utilized open datasets, while a smaller number relied on proprietary data. FL appears to be in its nascent phase, with open datasets predominantly used for initial testing purposes, such as performance validation. However, as the field matures and the volume of research utilizing authentic medical data grows, the utilization of proprietary data is expected to rise accordingly.

Most local models for medical FL research were neural networks, while very few were machine learning models. Considering that certain types of medical data, such as laboratory results, are captured in tabular formats that exhibit low data complexity [69-78], there is a need for FL research that utilizes machine learning. Machine learning models typically have lower complexity than neural network models and could be more suitable for these types of data.

We investigated neural network models and optimization methods. CNNs, the most widely utilized type of deep learning model, were employed in 35 out of 57 studies. The prevalent use of CNNs is likely due to the fact that image data were the most common type of data in these studies. Additionally, CNNs have been applied to the analysis of signal data [63,64,66]. The optimization method most frequently used was Adam, which was adopted in 35 studies. The application of Adam optimization was not limited to any particular data type; rather, it was employed across a broad range of data types. SGD was the optimization method used in 13 studies. Similar to Adam optimization, SGD was not predominantly used for any specific data types.

Moreover, we investigated the heterogeneity and security issues, which have been examined in many previous review papers. We found that although many algorithms have been proposed to address the issue of heterogeneity, there is still no low-cost, universally effective solution for all non-IID scenarios [98]. Given that FL in hospitals is a form of cross-silo FL with a limited number of clients, heterogeneity issues are more pronounced, necessitating further research.

Furthermore, we identified numerous security threats within FL, and measures such as differential privacy and homomorphic encryption have been proposed to mitigate these risks. Specifically, medical FL involves the use of patient data, which necessitates robust privacy and security safeguards. This makes it necessary to implement security enhancement measures, including differential privacy, to protect this sensitive information.

Currently, FL in the medical field is in its early stages, with a significant amount of research focusing on specific data types, such as imaging data, and particular diseases, such as cancer and COVID-19. As the field evolves, it is anticipated that FL will be applied to a broader range of data types and disease research. While many studies at present concentrate on open data, it is expected that the utilization of private data in research will grow in the future. Most FL local models in use today are based on neural networks. However, given the existence of tabular medical data, such as laboratory results, there is a potential for increased research into machine learning models, which typically have simpler structures than neural network models, for use as FL local models. As a result, medical FL research is poised to be actively pursued and is likely to become a critical component of collaborative research across multiple institutions.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgments

This work was supported by the Bio-Industrial Technology Development Program (No. 20014841), funded by the Ministry of Trade, Industry & Energy (MOTIE, Korea).

ORCID

Geunho Choi (https://orcid.org/0000-0003-2284-7619)
Won Chul Cha (https://orcid.org/0000-0002-2778-2992)
Se Uk Lee (https://orcid.org/0000-0003-4201-2272)
Soo-Yong Shin (https://orcid.org/0000-0002-2410-6120)

References

1. Shen D, Wu G, Suk HI. Deep learning in medical image analysis. Annu Rev Biomed Eng 2017;19:221-48. https://doi.org/10.1146/annurev-bioeng-071516-044442
2. Litjens G, Kooi T, Bejnordi BE, Setio AA, Ciompi F, Ghafoorian M, et al. A survey on deep learning in medical image analysis. Med Image Anal 2017;42:60-88. https://doi.org/10.1016/j.media.2017.07.005
3. European Union. General Data Protection Regulation [Internet]. Brussels, Belgium: European Union; c2023 [cited at 2024 Jan 31]. Available from: https://gdpr-info.eu/.
4. US Centers for Disease Control and Prevention. Health Insurance Portability and Accountability Act of 1996 (HIPAA) [Internet]. Atlanta (GA): Centers for Disease Control and Prevention; c2022 [cited at 2024 Jan 30]. Available from: https://www.cdc.gov/phlp/publications/topic/hipaa.html.
5. Korea Law Translation Center. Personal Information Protection Act (Act No. 16930, 2020) [Internet]. Sejong, Korea: Korea Law Translation Center; c2021 [cited at 2024 Jan 30]. Available from: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG.
6. Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, et al. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016 Oct 24-28; Vienna, Austria. p. 308-18. https://doi.org/10.1145/2976749.2978318
7. Dwork C.Differential privacy: a survey of results. In: Agrawal M, Du D, Duan Z, Li A, editors. Theory and applications of models of computation. Heidelberg, Germany: Springer; 2008. p. 1-19. https://doi.org/10.1007/978-3-540-79228-4_1
8. Goncalves A, Ray P, Soper B, Stevens J, Coyle L, Sales AP. Generation and evaluation of synthetic patient data. BMC Med Res Methodol 2020;20(1):108. https://doi.org/10.1186/s12874-020-00977-1
9. Chen RJ, Lu MY, Chen TY, Williamson DF, Mahmood F. Synthetic data in machine learning for medicine and healthcare. Nat Biomed Eng 2021;5(6):493-7. https://doi.org/10.1038/s41551-021-00751-8
10. Frid-Adar M, Diamant I, Klang E, Amitai M, Goldberger J, Greenspan H. GAN-based synthetic medical image augmentation for increased CNN performance in liver lesion classification. Neurocomputing 2018;321:321-31. https://doi.org/10.1016/j.neucom.2018.09.013
11. Naehrig M, Lauter K, Vaikuntanathan V. Can homomorphic encryption be practical? Proceedings of the 3rd ACM Workshop on Cloud Computing Security; 2011 Oct 21; Chicago, IL, USA. p. 113-24. https://doi.org/10.1145/2046660.2046682
12. Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys 2018;51(4):79. https://doi.org/10.1145/3214303
13. Fontaine C, Galand F. A survey of homomorphic encryption for nonspecialists. EURASIP J Inf Secur 2007;2007:13801. https://doi.org/10.1155/2007/13801
14. McMahan HB, Moore E, Ramage D, Hampson S, Arcas BA. Communication-efficient learning of deep networks from decentralized data [Internet]. Ithaca (NY): arXiv.org; 2023 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1602.05629.
15. Yoo JH, Jeong H, Lee J, Chung TM. Federated learning: issues in medical application [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2109.00202.
16. Pfitzner B, Steckhan N, Arnrich B. Federated learning in a medical context: a systematic literature review. ACM Trans Internet Technol 2021;21(2):50. https://doi.org/10.1145/3412357
17. Antunes RS, Andre da Costa C, Kuderle A, Yari IA, Eskofier B. Federated learning for healthcare: systematic review and architecture proposal. ACM Trans Intell Syst Technol 2022;13(4):54. https://doi.org/10.1145/3501813
18. Crowson MG, Moukheiber D, Arevalo AR, Lam BD, Mantena S, Rana A, et al. A systematic review of federated learning applications for biomedical data. PLOS Digit Health 2022;1(5):e0000033. https://doi.org/10.1371/journal.pdig.0000033
19. Nguyen DC, Pham QV, Pathirana PN, Ding M, Seneviratne A, Lin Z, et al. Federated learning for smart healthcare: a survey. ACM Comput Surv 2022;55(3):60. https://doi.org/10.1145/3501296
20. Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, et al. Advances and open problems in federated learning [Internet]. Ithaca (NY): arXiv.org; 2019 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1912.04977.
21. Li W, Milletari F, Xu D, Rieke N, Hancox J, Zhu W, et al. Privacy-preserving federated brain tumour segmen-

tation [Internet]. Ithaca (NY): arXiv.org; 2019 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1910.00962.

22. Sheller MJ, Edwards B, Reina GA, Martin J, Pati S, Kotrotsou A, et al. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Sci Rep 2020;10(1):12598. https://doi.org/10.1038/s41598-020-69250-1
23. Sarma KV, Harmon S, Sanford T, Roth HR, Xu Z, Tetreault J, et al. Federated learning improves site performance in multicenter deep learning without data sharing. J Am Med Inform Assoc 2021;28(6):1259-64. https://doi.org/10.1093/jamia/ocaa341
24. Jimenez-Sanchez A, Tardy M, Gonzalez Ballester MA, Mateus D, Piella G. Memory-aware curriculum federated learning for breast cancer classification. Comput Methods Programs Biomed 2023;229:107318. https://doi.org/10.1016/j.cmpb.2022.107318
25. Shen C, Wang P, Roth HR, Yang D, Xu D, Oda M, et al. Multi-task federated learning for heterogeneous pancreas segmentation [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2108.08537.
26. Misonne T, Jodogne S. Federated learning for heart segmentation. Proceedings of 2022 IEEE 14th Image, Video, and Multidimensional Signal Processing Workshop (IVMSP); 2022 Jun 26-29; Nafplio, Greece. p. 1-5. https://doi.org/10.1109/IVMSP54334.2022.9816345
27. Pati S, Baid U, Edwards B, Sheller M, Wang SH, Reina GA, et al. Federated learning enables big data for rare cancer boundary detection. Nat Commun 2022;13(1):7346. https://doi.org/10.1038/s41467-022-33407-5
28. Adnan M, Kalra S, Cresswell JC, Taylor GW, Tizhoosh HR. Federated learning and differential privacy for medical image analysis. Sci Rep 2022;12(1):1953. https://doi.org/10.1038/s41598-022-05539-7
29. Andreux M, Terrail JO, Beguier C, Tramel EW. Siloed federated learning for multi-centric histopathology datasets [Internet]. Ithaca (NY): arXiv.org; 2020 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2008.07424.
30. Lu MY, Chen RJ, Kong D, Lipkova J, Singh R, Williamson DF, et al. Federated learning for computational pathology on gigapixel whole slide images. Med Image Anal 2022;76:102298. https://doi.org/10.1016/j.media.2021.102298
31. Bercea CI, Wiestler B, Rueckert D, Albarqouni S. Feddis: disentangled federated learning for unsupervised brain pathology segmentation [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2103.03705.
32. Ke J, Shen Y, Lu Y. Style normalization in histology with federated learning. Proceedings of 2021 IEEE 18th International Symposium on Biomedical Imaging (ISBI); 2021 Apr 13-16; Nice, France. p. 953-6. https://doi.org/10.1109/ISBI48211.2021.9434078
33. Baid U, Pati S, Kurc TM, Gupta R, Bremer E, Abousamra S, et al. Federated learning for the classification of tumor infiltrating lymphocytes [Internet]. Ithaca (NY): arXiv.org; 2022 [cited at 2024 Jan 30]. https://doi.org/10.48550/arXiv.2203.16622
34. Lee H, Chai YJ, Joo H, Lee K, Hwang JY, Kim SM, et al. Federated learning for thyroid ultrasound image analysis to protect personal information: validation study in a real health care environment. JMIR Med Inform 2021;9(5):e25869. https://doi.org/10.2196/25869
35. Dayan I, Roth HR, Zhong A, Harouni A, Gentili A, Abidin AZ, et al. Federated learning for predicting clinical outcomes in patients with COVID-19. Nat Med 2021;27(10):1735-43. https://doi.org/10.1038/s41591-021-01506-3
36. Xu Y, Ma L, Yang F, Chen Y, Ma K, Yang J, et al. A collaborative online AI engine for CT-based COVID-19 diagnosis [Internet]. Ithaca (NY): arXiv.org; 2020 [cited at 2024 Jan 30]. Available from: https://doi.org/10.1101/2020.05.10.20096073.
37. Liu B, Yan B, Zhou Y, Yang Y, Zhang Y. Experiments of federated learning for COVID-19 chest X-ray images [Internet]. Ithaca (NY): arXiv.org; 2020 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2007.05592.
38. Zhang W, Zhou T, Lu Q, Wang X, Zhu C, Sun H, et al. Dynamic-fusion-based federated learning for COVID-19 detection. IEEE Internet Things J 2021;8(21):15884-91. https://doi.org/10.1109/JIOT.2021.305618
39. Feki I, Ammar S, Kessentini Y, Muhammad K. Federated learning for COVID-19 screening from chest X-ray images. Appl Soft Comput 2021;106:107330. https://doi.org/10.1016/j.asoc.2021.107330
40. Yang Q, Zhang J, Hao W, Spell GP, Carin L. FLOP: federated learning on medical datasets using partial networks. Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining; 2021 Aug 14-18; Virtual Event, Singapore. p. 3845-53. https://doi.org/10.1145/3447548.3467185

41. Cetinkaya AE, Akin M, Sagiroglu S. A communication efficient federated learning approach to multi chest diseases classification. Proceedings of 2021 6th International Conference on Computer Science and Engineering (UBMK); 2021 Sep 15-17; Ankara, Türkiye. p. 429-34. https://doi.org/10.1109/UBMK52708.2021.9558913
42. Dou Q, So TY, Jiang M, Liu Q, Vardhanabhuti V, Kaissis G, et al. Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study. NPJ Digit Med 2021;4(1):60. https://doi.org/10.1038/s41746-021-00431-6
43. Qayyum A, Ahmad K, Ahsan MA, Al-Fuqaha A, Qadir J. Collaborative federated learning for healthcare: multi-modal COVID-19 diagnosis at the edge. IEEE Open J Comput Soc 2022;3:172-84. https://doi.org/10.1109/OJCS.2022.3206407
44. Guo P, Wang P, Zhou J, Jiang S, Patel VM. Multi-institutional collaborations for improving deep learning-based magnetic resonance image reconstruction using federated learning. Proc IEEE Comput Soc Conf Comput Vis Pattern Recognit 2021;2021:2423-32. https://doi.org/10.1109/cvpr46437.2021.00245
45. Feng CM, Yan Y, Wang S, Xu Y, Shao L, Fu H. Specificity-preserving federated learning for MR image reconstruction. IEEE Trans Med Imaging 2023;42(7):2010-21. https://doi.org/10.1109/TMI.2022.3202106
46. Yang Z, Xia W, Lu Z, Chen Y, Li X, Zhang Y. Hypernetwork-based physics-driven personalized federated learning for CT imaging. IEEE Trans Neural Netw Learn Syst 2023 Dec 15 [Epub]. https://doi.org/10.1109/TNNLS.2023.3338867
47. Roth HR, Chang K, Singh P, Neumark N, Li W, Gupta V, et al. Federated learning for breast density classification: a real-world implementation [Internet]. Ithaca (NY): arXiv.org; 2020 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2009.01871.
48. Malekzadeh M, Hasircioglu B, Mital N, Katarya K, Ozfatura ME, Gunduz D. Dopamine: differentially private federated learning on medical data [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2101.11693.
49. Li X, Gu Y, Dvornek N, Staib LH, Ventola P, Duncan JS. Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results. Med Image Anal 2020;65:101765. https://doi.org/10.1016/j.media.2020.101765
50. Stripelis D, Ambite JL, Lam P, Thompson P. neuroscience research using federated learning. Proceedings of 2021 IEEE 18th International Symposium on Biomedical Imaging (ISBI); 2021 Apr 13-16; Nice, France. p. 1191-5. https://doi.org/10.1109/ISBI48211.2021.9433925
51. Liu D, Cabezas M, Wang D, Tang Z, Bai L, Zhan G, et al. Multiple sclerosis lesion segmentation: revisiting weighting mechanisms for federated learning. Front Neurosci 2023;17:1167612. https://doi.org/10.3389/fnins.2023.1167612
52. Linardos A, Kushibar K, Walsh S, Gkontra P, Lekadir K. Federated learning for multi-center imaging diagnostics: a simulation study in cardiovascular disease. Sci Rep 2022;12(1):3551. https://doi.org/10.1038/s41598-022-07186-4
53. Elayan H, Aloqaily M, Guizani M. Sustainability of healthcare data analysis IoT-based systems using deep federated learning. IEEE Internet Things J 2021;9(10):7338-46. https://doi.org/10.1109/JIOT.2021.3103635
54. Elayan H, Aloqaily M, Guizani M. Deep federated learning for IoT-based decentralized healthcare systems. Proceedings of 2021 International Wireless Communications and Mobile Computing (IWCMC); 2021 Jun 28-Jul 2; Harbin, China. p. 105-9. https://doi.org/10.1109/IWCMC51323.2021.9498820
55. Kassem H, Alapatt D, Mascagni P, Karargyris A, Padoy N. Federated cycling (FedCy): semi-supervised federated learning of surgical phases. IEEE Trans Med Imaging 2023;42(7):1920-31. https://doi.org/10.1109/TMI.2022.3222126
56. Agbley BL, Li J, Haq AU, Bankas EK, Ahmad S, Agyemang IO, et al. Multimodal melanoma detection with federated learning. Proceedings of 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP); 2021 Dec 17-19; Chengdu, China. p. 238-44. https://doi.org/10.1109/ICCWAMTIP53232.2021.9674116
57. Borger T, Mosteiro P, Kaya H, Rijcken E, Salah AA, Scheepers F, et al. Federated learning for violence incident prediction in a simulated cross-institutional psychiatric setting. Expert Syst Appl 2022;199:116720. https://doi.org/10.1016/j.eswa.2022.116720
58. Basu P, Roy TS, Naidu R, Muftuoglu Z, Singh S, Mireshghallah F. Benchmarking differential privacy and federated learning for BERT models [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arX-

iv.2106.13973.

59. Ge S, Wu F, Wu C, Qi T, Huang Y, Xie X. Fedner: privacy-preserving medical named entity recognition with federated learning [Internet]. Ithaca (NY): arXiv.org; 2020 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2003.09288.
60. Kanani P, Marathe VJ, Peterson D, Harpaz R, Bright S. Private cross-silo federated learning for extracting vaccine adverse event mentions [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2103.07491.
61. Sui D, Chen Y, Zhao J, Jia Y, Xie Y, Sun W. FedED: federated learning via ensemble distillation for medical relation extraction. Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP); 2020 Nov 16-20; Virtual Event. p. 2118-28.
62. Thwal CM, Thar K, Tun YL, Hong CS. Attention on personalized clinical decision support system: federated learning approach. Proceedings of 2021 IEEE International Conference on Big Data and Smart Computing (BigComp); 2021 Jan 17-20; Jeju, South Korea. p. 141-7. https://doi.org/10.1109/BigComp51126.2021.00035
63. Yoo JH, Son HM, Jeong H, Jang EH, Kim AY, Yu HY, et al. Personalized federated learning with clustering: non-IID heart rate variability data application [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2108.01903.
64. Zhang M, Wang Y, Luo T. (2020, December). Federated learning for arrhythmia detection of non-IID ECG. Proceedings of 2020 IEEE 6th International Conference on Computer and Communications (ICCC); 2020 Dec 11-14; Chengdu, China. p. 1176-80. https://doi.org/10.1109/ICCC51575.2020.9344971
65. Can YS, Ersoy C. Privacy-preserving federated deep learning for wearable IoT-based biomedical monitoring. ACM Trans Internet Technol 2021;21(1):21. https://doi.org/10.1145/3428152
66. Chen Y, Qin X, Wang J, Yu C, Gao W. Fedhealth: a federated transfer learning framework for wearable healthcare. IEEE Intell Syst 2020;35(4):83-93. https://doi.org/10.1109/MIS.2020.2988604
67. Wu Q, Chen X, Zhou Z, Zhang J. Fedhome: cloud-edge based personalized federated learning for in-home health monitoring. IEEE Trans Mob Comput 2020;21(8):2818-32. https://doi.org/10.1109/TMC.2020.3045266
68. Arikumar KS, Prathiba SB, Alazab M, Gadekallu TR, Pandya S, Khan JM, et al. FL-PMI: federated learning-based person movement identification through wearable devices in smart healthcare systems. Sensors (Basel) 2022;22(4):1377. https://doi.org/10.3390/s22041377
69. Rajendran S, Obeid JS, Binol H, D Agostino R Jr, Foley K, Zhang W, et al. Cloud-based federated learning implementation across medical centers. JCO Clin Cancer Inform 2021;5:1-11. https://doi.org/10.1200/CCI.20.00060
70. Choudhury O, Park Y, Salonidis T, Gkoulalas-Divanis A, Sylla I, Das AK. Predicting adverse drug reactions on distributed health data using federated learning. AMIA Annu Symp Proc 2020;2019:313-22.
71. Vaid A, Jaladanki SK, Xu J, Teng S, Kumar A, Lee S, et al. Federated learning of electronic health records to improve mortality prediction in hospitalized patients with COVID-19: machine learning approach. JMIR Med Inform 2021;9(1):e24207. https://doi.org/10.2196/24207
72. Jaladanki SK, Vaid A, Sawant AS, Xu J, Shah K, Dellepiane S, et al. Development of a federated learning approach to predict acute kidney injury in adult hospitalized patients with COVID-19 in New York City [Internet]. Cold Spring Harbor (NY): medRxiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.1101/2021.07.25.21261105.
73. Sadilek A, Liu L, Nguyen D, Kamruzzaman M, Serghiou S, Rader B, et al. Privacy-first health research with federated learning. NPJ Digit Med 2021;4(1):132. https://doi.org/10.1038/s41746-021-00489-2
74. Huang L, Shea AL, Qian H, Masurkar A, Deng H, Liu D. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. J Biomed Inform 2019;99:103291. https://doi.org/10.1016/j.jbi.2019.103291
75. Dang TK, Lan X, Weng J, Feng M. Federated learning for electronic health records. ACM Trans Intell Syst Technol 2022;13(5):72. https://doi.org/10.1145/3514500
76. Mondrejevski L, Miliou I, Montanino A, Pitts D, Hollmen J, Papapetrou P. FLICU: a federated learning workflow for intensive care unit mortality prediction. Proceedings of 2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS); 2022 Jul 21-23; Shenzen, China. p. 32-7. https://doi.org/10.1109/CBMS55023.2022.00013

77. Xu X, Peng H, Bhuiyan MZ, Hao Z, Liu L, Sun L, et al. Privacy-preserving federated depression detection from multisource mobile health data. IEEE Trans Ind Inf 2021;18(7):4788-97. https://doi.org/10.1109/TII.2021.3113708
78. Islam TU, Ghasemi R, Mohammed N. Privacy-preserving federated learning model for healthcare data. Proceedings of 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC); 2022 Jan 26-29; Las Vegas, NV, USA. p. 281-7. https://doi.org/10.1109/CCWC54503.2022.9720752
79. Kalra S, Adnan M, Taylor G, Tizhoosh H. Learning permutation invariant representations using memory networks [Internet]. Ithaca (NY): arXiv.org; 2019 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1911.07984.
80. Wang R, Fu B, Fu G, Wang M. Deep & cross network for Ad click predictions [Internet]. Ithaca (NY): arXiv.org; 2017 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1708.05123.
81. Albawi S, Mohammed TA, Al-Zawi S. Understanding of a convolutional neural network. Proceedings of 2017 International Conference on Engineering and Technology (ICET); 2017 Aug 21-23; Antalya, Türkiye. p. 1-6. https://doi.org/10.1109/ICEngTechnol.2017.8308186
82. Yu Y, Si X, Hu C, Zhang J. A review of recurrent neural networks: LSTM cells and network architectures. Neural Comput 2019;31(7):1235-70. https://doi.org/10.1162/neco_a_01199
83. Acheampong FA, Nunoo-Mensah H, Chen W. Transformer models for text-based emotion detection: a review of BERT-based approaches. Artif Intell Rev 2021;54:5789-829. https://doi.org/10.1007/s10462-021-09958-2
84. Kingma DP, Ba J. Adam: a method for stochastic optimization [Internet]. Ithaca (NY): arXiv.org; 2014 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1412.6980.
85. Ruder S. An overview of gradient descent optimization algorithms [Internet]. Ithaca (NY): arXiv.org; 2016 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1609.04747.
86. Wang Z, Song M, Zhang Z, Song Y, Wang Q, Qi H. Beyond inferring class representatives: user-level privacy leakage from federated learning. Proceedings of IEEE Conference on Computer Communications (INFOCOM); 2019 Apr 29-May 2; Paris, France. p. 2512-20. https://doi.org/10.1109/INFOCOM.2019.8737416
87. Luo X, Wu Y, Xiao X, Ooi BC. Feature inference attack on model predictions in vertical federated learning. Proceedings of 2021 IEEE 37th International Conference on Data Engineering (ICDE); 2021 Apr 19-22; Chania, Greece. p. 181-92. https://doi.org/10.1109/ICDE51399.2021.00023
88. Zhang J, Zhang J, Chen J, Yu S. GAN enhanced membership inference: a passive local attack in federated learning. Proceedings of 2020 IEEE International Conference on Communications (ICC); 52020 Jun 7-11; Dublin, Ireland. p. 1-6. https://doi.org/10.1109/ICC40277.2020.9148790
89. Hu H, Salcic Z, Sun L, Dobbie G, Zhang X. Source inference attacks in federated learning. Proceedings of 2021 IEEE International Conference on Data Mining (ICDM); 2021 Dec 7-10; Auckland, New Zealand. p. 1102-7. https://doi.org/10.1109/ICDM51629.2021.00129
90. Bhagoji AN, Chakraborty S, Mittal P, Calo S. Analyzing federated learning through an adversarial lens [Internet]. Ithaca (NY): arXiv.org; 2018 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1811.12470.
91. Fang M, Cao X, Jia J, Gong N. Local model poisoning attacks to Byzantine-Robust federated learning. Proceedings of the 29th USENIX Security Symposium; 2020 Aug 12-14; Boston, MA, USA p. 1605-22.
92. Tolpegin V, Truex S, Gursoy ME, Liu L. Data Poisoning Attacks Against Federated Learning Systems [Internet]. Ithaca (NY): arXiv.org; 2020 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2007.08432.
93. Zhang J, Chen J, Wu D, Chen B, Yu S. Poisoning attack in federated learning using generative adversarial nets. Proceedings of 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE); 2019 Aug 5-8; Rotorua, New Zealand. p. 374-80. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00057
94. Fung C, Yoon CJ, Beschastnikh I. Mitigating sybils in federated learning poisoning [Internet]. Ithaca (NY): arXiv.org; 2018 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1808.04866.
95. Liu P, Xu X, Wang W. Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives. Cybersecurity 2022;5(1):4. https://doi.org/10.1186/

s42400-021-00105-6

96. Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V. Federated optimization in heterogeneous networks [Internet]. Ithaca (NY): arXiv.org; 2018 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1812.06127.

97. Karimireddy SP, Kale S, Mohri M, Reddi SJ, Stich SU, Theertha Suresh A. Scaffold: stochastic controlled averaging for federated learning [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.1910.06378.

98. Li Q, Diao Y, Chen Q, He B. Federated learning on non-IID data silos: an experimental study [Internet]. Ithaca (NY): arXiv.org; 2021 [cited at 2024 Jan 30]. Available from: https://doi.org/10.48550/arXiv.2102.02079.

99. Fang H, Qian Q. Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet 2021;13(4):94. https://doi.org/10.3390/fi13040094

100. Park J, Lim H. Privacy-preserving federated learning using homomorphic encryption. Appl Sci 2022;12(2):734. https://doi.org/10.3390/app12020734

101. Timmis A, Vardas P, Townsend N, Torbica A, Katus H, De Smedt D, et al. European Society of Cardiology: cardiovascular disease statistics 2021. Eur Heart J 2022;43(8):716-99. https://doi.org/10.1093/eurheartj/ehab892

102. WHO CVD Risk Chart Working Group. World Health Organization cardiovascular disease risk charts: revised models to estimate risk in 21 global regions. Lancet Glob Health 2019;7(10):e1332-45. https://doi.org/10.1016/S2214-109X(19)30318-3

103. Dumurgier J, Tzourio C. Epidemiology of neurological diseases in older adults. Rev Neurol (Paris) 2020;176(9):642-8. https://doi.org/10.1016/j.neurol.2020.01.356

104. Gooch CL, Pracht E, Borenstein AR. The burden of neurological disease in the United States: a summary report and call to action. Ann Neurol 2017;81(4):479-84. https://doi.org/10.1002/ana.24897