INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
M. Kapkiç et al., Vol.12, No.1, pp. 21-31.
https://doi.org/10.55859/ijiss.1212964

Privacy Issues in Magnetic Resonance Images

Mahmut Kapkiç[1], Şeref Sağıroğlu[2]

[1]Computer Engineering Department, Atılım University, Ankara, Türkiye
[2] Computer Engineering Department, Gazi University, Ankara, Türkiye
Corresponding Author: mahmutkapkic@gmail.com

Research Paper Received: 01.12.2022 Revised: 15.01.2023 Accepted: 27.01.2023

Abstract—Privacy in magnetic resonance imaging (MRI) plays an important role due to violations occurring in scanning, storing, transferring, analyzing, and sharing. This paper reviews privacy concerns in MRI and especially Brain MRI in terms of datasets, models, platforms, violations, solutions used in privacy and security in the literature, discusses important issues based on risks, techniques, policies, rules, and existing and missing points in MRIs. Even if there have been rules, regulations, policies, and laws available for preserving privacy with the available techniques anonymization, differential privacy, federated learning, pseudonymization, synthetic data generation, privacy-utility or anonymization-utility dilemma is still on novel privacy-enhancing, or preserving techniques are always required to handle sensitive data with care. This paper focuses on these issues with some suggestions, and also discusses these issues for future directions.

Keywords—MRI privacy, privacy, security, review, datasets

1. Introduction

Many different systems are being developed for magnetic resonance images (MRIs) in healthcare. Examples of these systems can be given, such as improving MRI device capability, making the system automated, using artificial intelligence (AI) to support diagnoses and decision, increasing MRI resolution, accuracy and compression rates, and paying more attention to privacy and security, etc. If MRI devices are not properly managed or configured, they may result in privacy violations, security vulnerabilities, other undesirable or unexpected situations, or cases. In these systems, personal information identity (PII) and health status of patients may be revealed if privacy is not preserved, potentially damaging the reputation of individuals or institutions, may result in having fines due to legislations. The patient's personal information (such as Name, Age, Gender, Race, and Identity) and health status might be revealed if privacy is not preserved. For example, if data are not protected properly, there may be a leakage of data or violation of privacy. Violation of patients' privacy in the health may damage the reputation of a person or an institution.

Data sharing is an important issue in medical images and also in all digital media due to rising prominence of sharing and large-scale medical or non-medical studies. When brain MRI is considered, recognizing a person's identity from their faces, rendering or masking faces from brain MRIs are still under investigation due to the collected data to be considered re-identified, especially brain MRIs. Proper data anonymization, preserving data privacy, and respecting data privacy are now necessary due to national or international privacy acts and regulations such as the General Data Protection Regulation (GDPR).

There have been a number of studies that a person's identity or face might be still distinguished from rendering or masking in brain MRI images due to the possibility of re-identification of individuals from collected MRI data. In order to avoid this, one or more features of patients' name, date of birth, sex, age, type of illness or treatment, and so on is/are commonly removed from the datasets. There have been a number of regulations/acts in privacy and security issued for various sectors, such as the Health Insurance Portability and Accountability Act (HIPAA) for health, the Gramm-Leach-Bliley Act for finance, the Computer Fraud and Abuse Act (CFAA), and the Electronic Communication Privacy Acts (ECPA), Video Privacy Protection Acts (VPPA), NIST Cybersecurity Framework for transmission or stored information electronically, GDPR, KVKK (GDPR of Türkiye), and others. Especially, HIPAA [1] covers the following procedures for anonymizing collected patient data: removing "full-face photographs and any comparable images," and adhering to the five main rules: Privacy, Security, Transactions, Identifiers, and Enforcement. The Privacy rule protects the medical records of patients, limits the use of data without patient permission, allows patients to request corrections to their records, and gives every patient the right to know the details of their personal data. Violations of these rules can result in penalties. Despite the existence of numerous regulations, laws, studies, techniques, applications, and solutions for addressing privacy issues in MRI, the privacy-utility and anonymization-utility dilemma remains a challenge in the development of new privacy-enhancing or preserving techniques.

This paper is organized as follows. Section 2 describes techniques and methods used in preserving privacy in MRIs. Section 3 presents preserving privacy systems published in the literature and summarizes privacy issues published in MRI datasets. Section 4 introduces details of the Principles of Fair Privacy Rules and Practice in MRIs. In Section 5, the study is concluded with some criticism and discussion.

2. Techniques Used in MRI Privacy

Data privacy is a very important issue not only for health but also all sectors covering especially private or sensitive data. In order to protect data, e-health records are anonymized and achieved in the steps of preprocessing, ranking similar users, formation of equivalence classes, analysis of attribute classes, attribute classification, data anonymization, generalization, suppression, randomization, pseudonymization, bucketization, slicing, and cryptographic approaches [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. Looking at the articles reviewed on preserving privacy in MRIs, the proposed solutions used in the literature are summarized below:

De-identification [3], [4]: Brain MRIs often contain targeted brain images as well as images that reveal facial features, which can be used to re-identify individuals using facial recognition techniques and 3D modeling. This can be a privacy violation as it can disclose personal information. One solution to this issue is to remove or change parts of MRIs that are not necessary, such as using face masking, skull striping, or defacing methods. The defacing method involves focusing on and erasing or processing facial features such as the eyes, nose, or mouth, which play an important role in recognizing a familiar individual. When considering Brain MRIs specifically, there is a risk of re-identifying an individual by matching scans to identified photographs using face recognition. To preserve privacy in Brain

MRIs, a number of solutions exist in the literature, such as SPM-based methods, FreeSurfer, and FSL-based methods.

Cryptography [5], [6], [7]: Cryptography is a standardized security technique that prevents unauthorized access to patient data. When data is left in its raw form, it can be accessed and examined by anyone with access, which can cause privacy issues if the data is misused. To ensure that only authorized individuals can access and examine the data, the original data is transformed into meaningless data using a predetermined encryption algorithm, and the encrypted data is stored. If access to the original data is needed, the encrypted data can be decrypted using a technique.

Data Hiding [6], [8], [10]: In some system architectures, it is necessary to separate patients' data and images to ensure the security of both. To achieve this separation, data hiding techniques are used to integrate different data structures into a defined structure. These techniques can be divided into two methods: watermarking and steganography. Watermarking involves replacing the patient's data onto the image, and the embedded data can be either visible or invisible. The data can later be checked to ensure that the MR image was not distributed or violated by the original source (authenticity) or belongs to the correct patient (integrity). Steganography involves embedding the patient's data into the image data, and the data should be invisible.

Differential Privacy (DP) [11]: DP is a method of protecting data from inferring-linking attacks, which can potentially reveal sensitive information about individuals. DP can be also used to anonymize data in a structured way, such as by adding noise to the data or removing identifying rows/columns. These methods help to protect the privacy of individuals while still allowing for the analysis of the data.

Data Generation and Augmentation (DGA) [13]: DGA techniques are used for a variety of purposes, including respecting privacy and avoiding the use of real data that may violate individuals' privacy. Data augmentation is often used to increase the size of a small dataset by creating augmented versions of the data through techniques such as rotation and mirroring. Synthetic images, including Brain MRIs, can also be produced using techniques such as generative adversarial networks, image processing, or specific algorithms. These synthetic images can be used in place of real data to protect privacy while still allowing for analysis or experimentation.

Federated Learning (FLT) [9], [16], [17]: There are projects that use deep learning techniques to work with MRIs. However, sending the necessary information to a central processing center for these systems can pose privacy risks due to the centralization of the data. The FLT addresses this issue by decentralizing the deep learning process using multiple edge servers. With this technique, MRIs are interpreted using an iterative learning process. In this process, learning is first performed on edge servers using MRIs, and the resulting models are sent to a primary server. The primary server optimizes the models and then sends them to randomly selected edge servers. This allows for the development of a decentralized deep learning technique while still preserving privacy.

Decoy File [7]: One way to prevent the leakage of private information is to provide false information to attackers. This is a system that does not violate the privacy of the information obtained by the attacker and makes the attacker believe that the obtained information is correct. To create a decoy file, it should be made up of information that is independent of the information whose privacy is being preserved and does not contain any factual information. If the decoy file appears to be factual, it may reduce the likelihood of follow-on attacks by giving the attacker the impression that their goal has been achieved.

Synthetic Data Generation [12], [13]: It is possible to generate a large amount of data on a specific topic using a mathematical or statistical representation instead of using real data in analysis. In deep learning, using original MRIs for the training dataset can pose a risk to the privacy of the MRIs, as the security of the data may not be ensured if the MRIs are captured or retrieved from the model. To avoid violating the privacy of the MRIs, synthetic data can be produced that can serve the same function as the original data, but without any link to real data. This can help to preserve the privacy of the MRIs while still allowing for the use of the data in deep learning algorithms.

Randomized Order [5]: If an attacker gains access to a cloud server, they may be able to determine when files are uploaded, which can potentially lead to inferring-linking attacks. To prevent this issue, edge servers can cache files in a randomized order and then upload them to the cloud server. This can help to change the time metadata of the record time.

Medical Imaging Devices (MIDs) [14], [15]: Upon reviewing the literature, it appears that there have been relatively few publications focusing on privacy violations in the context of MIDs. However, as noted in [14], MIDs are vulnerable to cyber attacks due to their connections to hospital networks or the internet. These attacks can target devices, infrastructure, and components through methods such as Configuration Files Disruption, Mechanical Disruption of MID's Motors, Disruption of Image Results, and Ransomware DoS, and can be sophisticated enough to destroy patient records and violate privacy [14].

3. Principles of Fair Privacy Rules and Practice for MRIs

There have been numerous solutions proposed in the literature for addressing data security and privacy in the context of MRI [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [26], [27], [28], [29], [30], [31], [23], [24], [25], [16], [17], [14]. Based on these reviews, several privacy rules and practices have been suggested for MRI, which are largely drawn from [1] and include the following:

3.1. Data Collection Limits

It is important to clarify the policies for data collection time, which will depend on the purposes for holding the data. Personal data should not be kept for longer than necessary and should be periodically reviewed and anonymized or erased [28]. In the case of MRI data, which are typically collected in NIFTI or DICOM format and have specific formats for pixel depth, photometric interpretation, metadata, and pixel data, there may be limitations on the quality of the data due to device configurations.

3.2. Data Quality Expectation

According to the GDPR Article 16, individuals have the right to obtain the rectification of inaccurate personal data and to have incomplete personal data completed. High-quality images are also necessary for effective data analysis and interpretation. While current image quality is generally good, there are still datasets available with different memory sizes and formats.

3.3. Data Specification for Specific Purposes

It is important to define clear policies for the purposes of processing MRI data, as the data is very

Table 1.
Privacy issues literature

Ref	Model	Platform	Dataset	Privacy	Security	Others
[3]	N/A	Portable System	LocalizeMI, IXI	De-identification with AnonyMI Algorithm	N/A (Not Applicaple)	According to averages of participatory experiments are; 33% for AnonyMI, 35% for Maskface, and 29% for PyDeface. Source localization results with the original MRIs are; 88% for AnonyMI, 85% for Maskface, and 84% for PyDeface.
[4]	N/A	Portable System	ADNI, MAGNIMS, the PICTURE project	De-identification	N/A	Automated analysis methods failed in 0–19% of cases in Facial Features Removal processed images versus 0–2% of cases in full images; Intra-class correlation coefficient for absolute agreement ranged from 0.312 to 0.998.
[5]	N/A	Cloud	N/A	Randomized Order, Encryption	N/A	N/A
[6]	N/A	Portable System	MammographIC Image Analysis Society	Steganography, Encryption	AES256 Encryption	MSE value decreased to 0.00257 from 0.0259; High Peak Signal to Noise Ratio increased to 78.79652 from 63.06; No loss.
[7]	N/A	Cloud	N/A	Decoy File System, Encryption	User Profiling for Authentication	At the end, two galleries are generated. Actual images are kept secretly in the cloud, and decoy files are kept as a honeypot in the fog. Unauthorized accesses will redirect to decoy files. Actual images are only accessible by a user after verifying their authenticity.
[9]	CNN	Multi-Platform	MNIST, CIFAR10, Organ MNIST, PathMNIST	FedSLD	N/A	Federated Learning with Shared Label Distribution (FedSLD) improved on Accuracy value ranging from 1.10% to 5.50%. The improvement of Best Test Accuracy ranging from 0.18% to 2.41% for FedAvg and FedProx algorithms.
[10]	N/A	Portable System	N/A	Watermarking with Histogram Strategy	N/A	Improved the embedding capacity by 68.44% on average
[11]	ICA	Portable System	Human Connectome Project	DI with Correlation Assisted Private Estimation	N/A	N/A
[12]	U-Net	Portable System	Human Connectome Project, WU-Minn Consortium	Synthetic Data Generation	N/A	Lindner et al.'s synthetic GBM data on classification results: Dice coefficient of 86.197%. Hausdorff distance of 5.780. Sensitivity:80.237%; Specificity:99.988%.
[13]	PG-GAN, U-net	Portable System	N/A	Synthetic Data Generation with PG-GAN	N/A	According to the experiment done with cardiac magnetic resonance (CMR) experts and non-CMR specialists. Recognizing PG-GAN are 68.7% for non-CMR specialists and 72.2% for CMR experts.
[18]	N/A	Portable System	Medical Image Samples by S. Barre	Watermarking	N/A	Compared with 11 different watermarking methods, most of the results have a better value in themselves.

specific and may require preprocessing for analysis, security, or privacy [29].

Table 2.
Violations of privacy issues and approaches in datasets

Ref	Description	Violations in Privacy Issues	Privacy Approach
[19]	319 patients' brain MRI. Age, Gender data are given per patient.	Faces are identifiable. Linkability with age and gender data.	Anonymization
[20]	64 patients' brain MRI; Contain 24 males, 16 females, and uniformed 24 people; Age percentages are given.	N/A	Skull stripping, Anonymization
[21]	242 patients' brain MRI; Contain 95 males and 147 females; Median age: 56, range: 24-84.	N/A	Anonymization, Face masking.
[22]	1370 patients' brain MRI; Age, Gender, Sexual orientation, Body-Mass index, Handedness, Educational level/category, Socio-economic status, Religion, and Psychometric variables are given per patient.	Linkability	Skull stripping, anonymization.
[23]	1271 patients' brain MRI.	N/A	Skull stripping; Anonymization
[24]	243 patients' brain MRI.	N/A	Skull stripping; Anonymization
[25]	100 patients' brain MRI. Contain 50 HGG, 50 normal. 12 features such as Age, Gender, Sex, etc. are given per patient.	N/A	Skull stripping, Anonymization, Defacing

3.4. Data Limits in Uses

According to the GDPR Article 5, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization). MRI data are used for specific purposes with intensive care. Especially, linkages and patients' permissions for data use might limit studies and applications. This certainly depends on the patients' permissions, privacy acts, and specific rules based on specific purposes.

3.5. Data Security and Privacy Approaches

Data confidentiality, integrity, and availability, should be ensured by considering the system's security based on; managing security risk, protecting personal data against cyber-attack, detecting security events, and minimizing the impact [30]. Even if there are available techniques in the literature to provide security and privacy, more attention is required to handle security and privacy issues.

3.6. Open Access Data Availability

According to the GDPR, open data sharing is lawful under certain conditions specified in Article 6(e)(f): ”processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.” While open access MRI data sets are available in the literature, applying privacy-preserving techniques to these data sets may reduce their utility.

3.7. Data Rights Management for Individuals

The rights of individuals as outlined in the GDPR Chapter 3 include the right to be informed, access, rectification, erasure, restriction of processing, data portability, object, automated individual decision-making, and profiling. These issues are particularly important to consider when dealing with MRI data. While data obtained from patients may be used with their permission, it is important to manage and respect these permissions.

3.8. Data Accountability

The GDPR also emphasizes accountability in Article 5(2), stating that ”the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability).” This helps to ensure that privacy and security issues are taken seriously in the context of MRI.

4. Conclusion and Discussion

This paper presents a review on privacy issues, rules, techniques and concerns on medical images, especially in Brain MRIs. Based on the studies, reviews and suggestions, and summaries in Tables 1 and 2, there have also been a number of issues to be criticized and evaluated below as:

- Health data is very sensitive and requires special attention, treatments, processes, and care for KVKK, GDPR or Privacy Acts. Any violation should be subject to legal obligations. This makes data owners not to share or to do any analysis on data even if there have been available solutions for data anonymization in the literature as introduced to ensure data privacy and security. Another way of saying, there have been enough support and available solutions to handle MRI datasets for preserving privacy issues with privacy acts, laws, rules, techniques, or solutions.

- Available privacy acts such as HIPAA, CFAA, ECPA, GDPR, KVKK provide good solutions, rules and frameworks for preserving privacy. In addition, as suggested in Section 4, Principles of Fair Privacy Rules and Practice will be followed supporting privacy not only in MRIs but also in other medical images. As reported in [17], MRI datasets might be standardized for better security and privacy.

- Data utility-privacy, utility-anonymization, quality-quantity, and security-privacy-cost are the recent dilemmas to be considered more for supporting security and privacy issues more than ever. Respecting privacy and getting value from data are the main problem and very important not only for developing new products or outputs but also for all other research fields. Likely, as introduced available techniques and solutions in this article, more commitments are required for patients’ data in research activities and progresses, privacy-preserving, security rules and measures, auditing, policy-making, etc.

- The balance between privacy and utility is also important in developing new privacy-enhancing and preserving techniques. Striking a balance among these two goals can be a challenge, and require more attention for different applications. Recent achievements and results have shown that there are improvements in having utility using available techniques introduced in this article but better results are always required.

- Considering the potential for cyberattacks and other security threats in the handling of medical image data is also critical and essential to have robust security measures in place to protect against these threats and attacks.

- Even if there have been many methods or techniques to support privacy and security issues such as privacy-enhancing or preserving techniques cryptography, steganography, anonymization, DP, DGA, FLT, pseudonymization, data generation, etc. there are still required to new methods and techniques based on the vulnerability statistics in the literature.

- Even if security and privacy issues are being supported by researchers, scientists or data collectors declaring clearly how and why private data are collected, and used in the studies, the reality has shown that there are still violations and vulnerabilities in health studies, applications and implementations.

- Watermarking and steganographic privacy solutions also give different perspectives to support not only privacy but also integrity and authenticity. More attention should be paid for this type of solutions.

- Recent violations and vulnerabilities have shown that cyber-attacks on MIDs are crucial and become a major challenge for device manufacturers, healthcare providers, hospitals, or researchers. In order to ensure a secure MIDs, and protect and preserve patients' data, more attention is required to understand violations, system vulnerabilities, potential attacks, and risks to develop better and tighter secure and privacy-aware solutions.

- As reported in [32], legal and ethical challenges in medical big data bring to patients' privacy in front be discussed more on "how best to conceive of health privacy; the importance of equity, consent, and patient governance in data collection; discrimination in data uses; and how to handle data breaches".

- More specifically, de-identification in DICOM data is also essential to preserve the privacy of patients' personally identifiable information. Recent studies have shown that de-identification process of DICOM attributes is important and some of them are required to be removed. Likely, a two-stage de-identification process for medical images is available in DICOM file format [33]. This process must be taken into account in establishing further datasets.

- As indicated in [34], Medical Imaging in Internet of Things (MIIoT) now is a recent trend toward improving health devices and services by offering smooth and better medical facilities. Security and privacy issues in MIIoT devices and technologies are also growing interest and crucial topics for the near future. So, more attention is required for more and tight privacy solutions in terms of accessing, storing, analyzing, transferring, and authorizing solutions.

- There are also obstacles in reality to data sharing. Not all researchers are supportive of data sharing due to recent and emerging regulations, penalties, difficulty in having permissions, keeping data themself for publications, lack of knowledge, excuses with many other things, etc. As stated in [35], "there should be a balance, as keeping data under lock and key for use by only a handful of researchers may protect privacy, but will limit scientific discovery. Alternatively, sharing everything with everyone does not safeguard individual privacy". If open science or open access dataset's philosophy is extended, this will be brought to trial and solve many problems and getting more value from datasets.

- Establishing more training programs at the universities such as "data analytics", "data security" "data privacy", "data science", and "responsible AI" are good attempts to support privacy and security issues more carefully.

- Privacy in MRI datasets is necessary for organizations to comply with national and international regulations if it is being developed a real application or a product to preserve patients' data and to increase customers' or users' confidence. Without doing so, a developed system or product will be at risk, and services will be approached to suspicion. Any system should be developed based on security and privacy concerns for further businesses.

- As reported in Turkish Brain Project [24], the project creates an open-access brain MRI dataset (GaziBrain2020) covering all steps of privacy concerns such as masking and deleting personal information, cleaning metadata from DICOM, anonymization, and defacing processes. With the help of this dataset, daily or instant MRI analysis using deep learning models for disease, tumor and anomaly detection or other issues are achieved in accordance with the tasks. As a result of this, publishing privacy preserving open access datasets are very important to develop new privacy-aware algorithms and to do better and more accurate studies and applications as well as other fields.

- Finally, our experience from Turkish Brain Project [24] has shown that; working with our own data is a real experience and requiring more attention than using benchmark datasets available in the literature; ensuring privacy in MRI dataset is also crucial for protecting the privacy of patients, maintaining their trust, and also respecting their privacy based on KVKK in the project is also very good experiences; doing a real project, preparing all agreement documents among partner institutions, explaining them what is done, showing respect in reality on the sides and documents, finally making all partners happy are really fantastic experiences; preparing GaziBrain2020 dataset, applying anonymization, masking and filtering techniques to the dataset, and publishing it are also a very good experience and responsibility to be able to securely and ethically handle sensitive medical information.

Acknowledgment

This paper was prepared as part of the Turkish Brain Project (No: 2021-001) supported by the Digital Transformation Office (DDO) of the Presidency of Turkey. The authors would like to express their gratitude to the DDO for their financial support and to the Gazi University (GU) Medical School Hospital for providing facilities for the project. The authors would also like to specifically thank the Office Head, Dr. Ali Taha KOÇ, and the Rector of GU, Prof. Dr. Musa YILDIZ, for their special support, as well as the colleagues from the Office and the University.

References

[1] The US Department of Health and Human Services (HSS). Methods for de-identification of PHI. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html. Accessed: 21.02.2023.

[2] A. Majeed, “Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data,” *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 4, p. 426–435, 2019.

[3] E. Mikulan, S. Russo, F. M. Zauli, P. d’Orio, S. Parmigiani, J. Favaro, W. Knight, S. Squarza, P. Perri, F. Cardinale, P. Avanzini, and A. Pigorini, “A comparative study between state-of-the-art mri de-identification and anonymi, a new method combining re-identification risk reduction and geometrical preservation,” *Human Brain Mapping*, vol. 42, no. 17, p. 5523–5534, 2021.

[4] A. De Sitter, M. Visser, I. Brouwer, K. Cover, R. van Schijndel, R. Eijgelaar, D. Müller, S. Ropele, L. Kappos, Á. Rovira *et al.*, “Facing privacy in neuroimaging: Removing facial features degrades performance of image analysis methods ,” *European Radiology*, vol. 30, no. 2, p. 1062–1074, 2019.

[5] J. Vincent, W. Pan, and G. Coatrieux, “Privacy protection and security in eHealth Cloud Platform for medical image sharing,” *2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, 2016.

[6] S. Khalifeh, J. Georgi, and S. Shakhatreh, “Design and implementation of a steganography-based system that provides protection for breast cancer patient’s data,” *2022 56th Annual Conference on Information Sciences and Systems (CISS)*, 2022.

[7] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, “A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography,” *IEEE Access*, vol. 5, p. 22313–22328, 2017.

[8] S. M. Mousavi, A. Naghsh, and S. Abu-Bakar, “Watermarking techniques used in medical images: A survey,” *Journal of Digital Imaging*, vol. 27, no. 6, p. 714–729, 2014.

[9] J. Luo and S. Wu, “Fedsld: Federated Learning with Shared Label Distribution for Medical Image Classification,” *2022 IEEE 19th International Symposium on Biomedical Imaging (ISBI)*, 2022.

[10] M.-H. Wu, J. Zhao, B. Chen, Y. Zhang, Y. Yu, and J. Cheng, "Reversible data hiding based on medical image systems by means of histogram strategy," *2018 3rd International Conference on Information Systems Engineering (ICISE)*, 2018.

[11] H. Imtiaz, J. Mohammadi, R. Silva, B. Baker, S. M. Plis, A. D. Sarwate, and V. D. Calhoun, "A correlated noise-assisted decentralized differentially private estimation protocol, and its application to fmri source separation," *IEEE Transactions on Signal Processing*, vol. 69, p. 6355–6370, 2021.

[12] L. Lindner, D. Narnhofer, M. Weber, C. Gsaxner, M. Kolodziej, and J. Egger, "Using synthetic training data for Deep Learning-based GBM segmentation," *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2019.

[13] G.-P. Diller, J. Vahle, R. Radke, M. L. B. Vidal, A. J. Fischer, U. M. Bauer, S. Sarikouch, F. Berger, P. Beerbaum, H. Baumgartner *et al.*, "Utility of deep learning networks for the generation of artificial cardiac magnetic resonance images in congenital heart disease," *BMC Medical Imaging*, vol. 20, no. 1, 2020.

[14] T. Mahler, N. Nissim, E. Shalom, I. Goldenberg, G. Hassman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahar, "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices," *arXiv.org*, 2018. [Online]. Available: https://arxiv.org/abs/1801.05583

[15] Rebekah Moan. Report: 45m medical images are accessible online. https://www.auntminnie.com/index.aspx?sec=sup&sub=pac&pag=dis&ItemID=131133. Accessed: 14.08.2022.

[16] M. R. Cohen. A legal guide to privacy and data security. https://www.leg.mn.gov/docs/2019/other/190030.pdf. Accessed: 14.08.2022.

[17] A. E. Cetinkaya, M. Akin, and S. Sagiroglu, "A communication efficient federated learning approach to multi chest diseases classification," *2021 6th International Conference on Computer Science and Engineering (UBMK)*, pp. 429–434, 15-17 Sep 2021.

[18] R. Tamilselvi, A. Nagaraj, M. P. Beham, and M. B. Sandhiya, "Bramsit: A database for brain tumor diagnosis and detection," *2020 Sixth International Conference on Bio Signals, Images, and Instrumentation (ICBSII)*, 2020.

[19] A. Sayah, C. Bencheqroun, K. Bhuvaneshwar, A. Belouali, S. Bakas, C. Sako, C. Davatzikos, A. Alaoui, S. Madhavan, and Y. Gusev, "Enhancing the Rembrandt MRI collection with expert segmentation labels and Quantitative Radiomic features," *Scientific Data*, vol. 9, no. 1, 2022.

[20] J. Shapey, A. Kujawa, R. Dorent, G. Wang, A. Dimitriadis, D. Grishchuk, I. Paddick, N. Kitchen, R. Bradford, S. R. Saeed *et al.*, "Segmentation of vestibular schwannoma from MRI, an open annotated dataset and Baseline Algorithm," *Scientific Data*, vol. 8, no. 1, 2021.

[21] L. Snoek, M. M. van der Miesen, T. Beemsterboer, A. Van Der Leij, A. Eigenhuis, and H. Steven Scholte, "The Amsterdam open MRI collection, a set of multimodal MRI datasets for individual difference analyses," *Scientific Data*, vol. 8, no. 1, 2021.

[22] S.-L. Liew, B. P. Lo, M. R. Donnelly, A. Zavaliangos-Petropulu, J. N. Jeong, G. Barisano, A. Hutton, J. P. Simon, J. M. Juliano, A. Suri *et al.*, "A large, curated, open-source stroke neuroimaging dataset to improve lesion segmentation algorithms," *Scientific Data*, vol. 9, no. 1, 2022.

[23] S. Bakas, H. Akbari, A. Sotiras, M. Bilello, M. Rozycki, J. S. Kirby, J. B. Freymann, K. Farahani, and C. Davatzikos, "Advancing the cancer genome Atlas Glioma MRI collections with expert segmentation labels and Radiomic features," *Scientific Data*, vol. 4, no. 1, 2017.

[24] D. T. O. of the Presidency of Turkey. Turk brain project. https://cbddo.gov.tr/en/projects/turkish-brain-project/. Accessed: 14.08.2022.

[25] European Parliament Official Legal Text. General data protection regulation (gdpr). https://gdpr-info.eu/. Accessed: 14.08.2022.

[26] L. Xiang, "Survey on privacy preserving techniques for publishing social network data," *Journal of Software*, vol. 25, p. 576–590, 2014.

[27] European Society of Radiology (ESR), "The new eu general data protection regulation: What the radiologist should know," *Insights into Imaging*, vol. 8, no. 3, p. 295–299, 2017.

[28] Information Commissioner's Office (ICO). Principle (e): Storage limitation. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation. Accessed: 14.08.2022.

[29] ICO- Information Commissioner's Office. Principle (b): Purpose limitation. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/. Accessed: 14.08.2022.

[30] Information Commissioner's Office (ICO). Security outcomes. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/security-outcomes/. Accessed: 14.08.2022.

[31] S. M. Mousavi, A. Naghsh, A. A. Manaf, and S. Abu-Bakar, "A robust medical image watermarking against salt and pepper noise for Brain MRI images," *Multimedia Tools and Applications*, vol. 76, no. 7, p. 10313–10342, 2016.

[32] T. White, E. Blok, and V. D. Calhoun, "Data sharing and privacy issues in neuroimaging research: Opportunities, obstacles, challenges, and monsters under the bed," *Human Brain Mapping*, vol. 43, no. 1, p. 278–291, 2020.

[33] A. Shahid, M. H. Bazargani, P. Banahan, B. Mac Namee, T. Kechadi, C. Treacy, G. Regan, and P. MacMahon, "A two-stage de-identification process for privacy-preserving medical image analysis," *Healthcare*, vol. 10, no. 5, p. 755, 2022.

[34] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe, and A. Welhenge, "Security and privacy issues in medical internet of things:

Overview, countermeasures, challenges and future directions," *Sustainability*, vol. 13, no. 21, p. 11645, 2021.

[35] M. Bezzi and J.-C. Pazzaglia, "The anonymity vs. utility dilemma," *ISSE 2008 Securing Electronic Business Processes*, p. 99–107, 2009.