World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:18, No:7, 2024

# Methods and Algorithms of Ensuring Data Privacy in AI-Based Healthcare Systems and Technologies

Omar Farshad Jeelani, Makaire Njie, Viktoriia M. Korzhuk

***Abstract*****—**Recently, the application of AI-powered algorithms in healthcare continues to flourish. Particularly, access to healthcare information, including patient health history, diagnostic data, and PII (Personally Identifiable Information) is paramount in the delivery of efficient patient outcomes. However, as the exchange of healthcare information between patients and healthcare providers through AI-powered solutions increases, protecting a person's information and their privacy has become even more important. Arguably, the increased adoption of healthcare AI has resulted in a significant concentration on the security risks and protection measures to the security and privacy of healthcare data, leading to escalated analyses and enforcement. Since these challenges are brought by the use of AI-based healthcare solutions to manage healthcare data, AI-based data protection measures are used to resolve the underlying problems. Consequently, these projects propose AI-powered safeguards and policies/laws to protect the privacy of healthcare data. The project present the best-in-school techniques used to preserve data privacy of AI-powered healthcare applications. Popular privacy-protecting methods like Federated learning, cryptography techniques, differential privacy methods, and hybrid methods are discussed together with potential cyber threats, data security concerns, and prospects. Also, the project discusses some of the relevant data security acts/laws that govern the collection, storage, and processing of healthcare data to guarantee owners' privacy is preserved. This inquiry discusses various gaps and uncertainties associated with healthcare AI data collection procedures, and identifies potential correction/mitigation measures.

***Keywords*****—**Data privacy, artificial intelligence, healthcare AI, data sharing, healthcare organizations.

## I. Introduction

ARTIFICIAL intelligence (AI) is the ability of machines (computers) to discharge duties similar to ones humans perform. Simply put, AI stimulates human-like intelligence through computer software imitating human activities artificially. Nevertheless, AI demands a huge volume of data and computing power to achieve its full capacity. Whereas computing power has certainly helped to revive AI, data has undoubtedly enabled this technology to accomplish all its immediate successes [1]. Lately, AI-enabled software solutions have had progressive adoption. Remarkably, AI has become a factor standard/method for processing huge volumes of data to facilitate complex decisions that are not only hard but also impossible for humans to make in some fields. This is because the large amounts of data (also referred to as big data) generated today substantially surpass human capability to use, understand, and-consume [2].

In healthcare, there has been a progressive adoption of AI-powered solutions. As of 2021, only one-fifth of healthcare providers globally who were surveyed showed substantial adoption of AI models in their data architecture, and natural language processing (NLP) was reported as the most used AI-enabled solution. The globe's market size for healthcare AI during this period was USD 11.06 billion. In 2023, the market size rose to USD 20.65 billion and it is projected to hit approximately USD 188 billion in 2030 [3].

AI-powered healthcare systems/procedures imply integrating AI algorithms and technologies into different disciplines of the healthcare sector. AI-enabled healthcare systems leverage the power of artificial intelligence to analyze huge volumes of healthcare data, generate useful insights, and help healthcare stakeholders to make informed decisions. These systems encompass a vast variety of use cases, such as personalized treatment, medical disease diagnosis and detection, predictive analytics, healthcare bots, and virtual assistant among others.

AI technologies used in healthcare systems include machine learning (ML), deep learning (DL), computer vision, and NLP. The methods are to handle, manage, analyze, and interpret healthcare data, like medical images, genomics, sensor information, electronic health records (EHRs), and patient-generated information. AI-driven healthcare systems analyze patterns, identify correlations, and learn from vast datasets to improve health outcomes, increase efficiency, and provide individualized patient care [4].

Recently, there has been tremendous advancement in healthcare AI and these advances will shortly have a substantial real-life impact. Numerous novel AI-powered healthcare technologies are nearing viability and a handful have been integrated into health systems [5]. For instance, AI has proven to be particularly helpful in diagnostic imagery analysis. In a recent study, scientists at Stanford developed an AI algorithm that could decode chest X-rays for fourteen different pathologies in barely a few seconds [6]. Other healthcare specialties, including robotic operation, radiation oncology, and organ allocation among others are markedly impacted by AI advancements [7]. However, owing to this rapid growth, there is an escalating public discourse about the benefits and dangers of artificial intelligence and how to control its advancement [8].

Omar Farshad Jeelani, PhD student, Makaire Njie, PhD student, and Viktoriia M. Korzhuk, Associate Professor, are with the ITMO University in Saint Petersburg, Russia (e-mail: omar@itmo.ru, mnjie@itmo.ru, vmkorzhuk@itmo.ru).

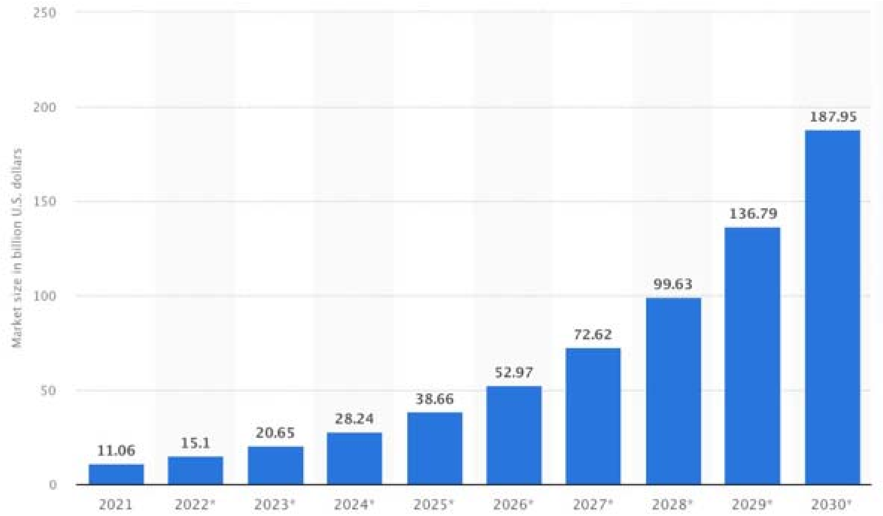

Fig. 1 Healthcare AI market size globally (2021-2030) [3]

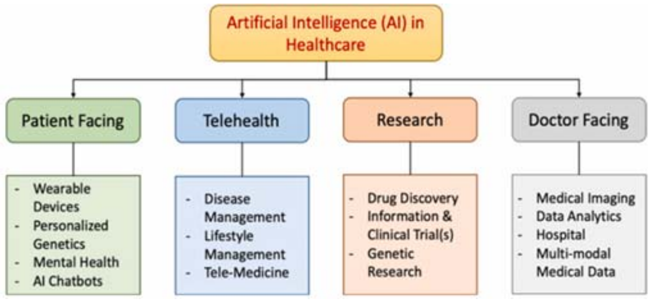

Fig. 2 Applications of healthcare AI

AI-powered healthcare techniques, nevertheless, inherently require vast amounts of training data, thus securing patient data is essentially important to implement any research affiliated with AI [9]. Whereas there is presently no centralized standard (protocol) for the implementation of data encryption as well as sharing for AI-driven study, the protocols are decided from a personal project standpoint after accreditation from an ethical perspective by the relevant institutional ethics authority. For instance, if anonymized patient diagnosis data is used to conduct retrospective AI-based research, informed patient willingness may be forfeited if found legitimate by an ethics committee. Also, there are myriads of non-proprietary large healthcare data repositories such as TCIA (The Cancer Imaging Archive) that can freely be accessed by the public and also used for AI-oriented research to develop systemized protocols and reproducible outcomes. Optimum and DDSM (Digital Database for Screening Mammography) are popular open-source databases that contain carefully curated mammographic images often deployed to train and test DL algorithms [10].

### *A. Importance of Data Privacy and Security in AI-Driven Healthcare Systems*

Data security and privacy are critically important in AI-driven healthcare systems, as they offer:

- Patient confidentiality: AI-driven healthcare systems ensure the protection of patient confidentiality through privacy safeguards. Sensitive, valuable patient information such as medical records, real-time monitoring information, and genetic information among others should be managed with great care [11]. Preserving patient privacy helps respect not only their right to privacy but also bolsters trust between them and healthcare organizations.
- Information security: AI-driven healthcare systems leverage huge amounts of patient information. This information is susceptible to security breaches, manipulation, unauthorized access, and damage by hackers, malicious users, or disgruntled employees [12]. Security measures such as data encryption, secure storage, firewall protection, and access controls are important to safeguard patient data against infringement and guarantee data integrity.
- Informed consent: AI-driven healthcare systems usually require constant access to medical information for analysis and decision-making. Enabling patient privacy and granting them autonomy over their data necessitates obtained consent to gather, store, and consume their data [13]. Transparent and comprehendible communication of how patient information will be used is important to ensure that data owners (patients) have control over their valuable information and allow them to make informed decisions regarding its consumption.
- Secondary consumption of data: valuable patient information gathered for AI training has implications beyond conventional patient care. The data may be used to conduct research or perform public health initiatives. Privacy safeguards are important in controlling the secondary consumption of information, ensuring compliance with ethics, and preventing unauthorized exploitation or divulgence of patient data.
- Reducing/mitigating bias and discrimination: healthcare AI algorithms can be vulnerable to prejudice that leads to discriminatory or unjust outcomes. Data privacy and security play a critical role in ensuring that the training data used to train the AI models is diverse, anonymized, as well as representative hence mitigating the biases. Ultimately,

this promotes equitable and impartial delivery of health care.

- Regulatory compliance: HCOs should comply with data security regulations, like the EU's General Data Protection Regulation (GDPR), IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS), and US's Health Insurance Portability and Accountability Act of 1996 (HIPAA). While complying with these data protection laws is a legal obligation, it helps guarantee the secure handling of patient data, and a way that respects their right to privacy [14].
- Preserves public trust: Undoubtedly, breach of privacy and misuse of information erodes public confidence in AI-driven healthcare systems. Putting in place study data protection and privacy measures is crucially important as it helps bolster public confidence in a healthcare sector that adopts AI solutions. Clear data processing practices and good communication concerning the protection of patient privacy immensely contribute to building trust between healthcare givers, AI-driven healthcare technologies, and patients.

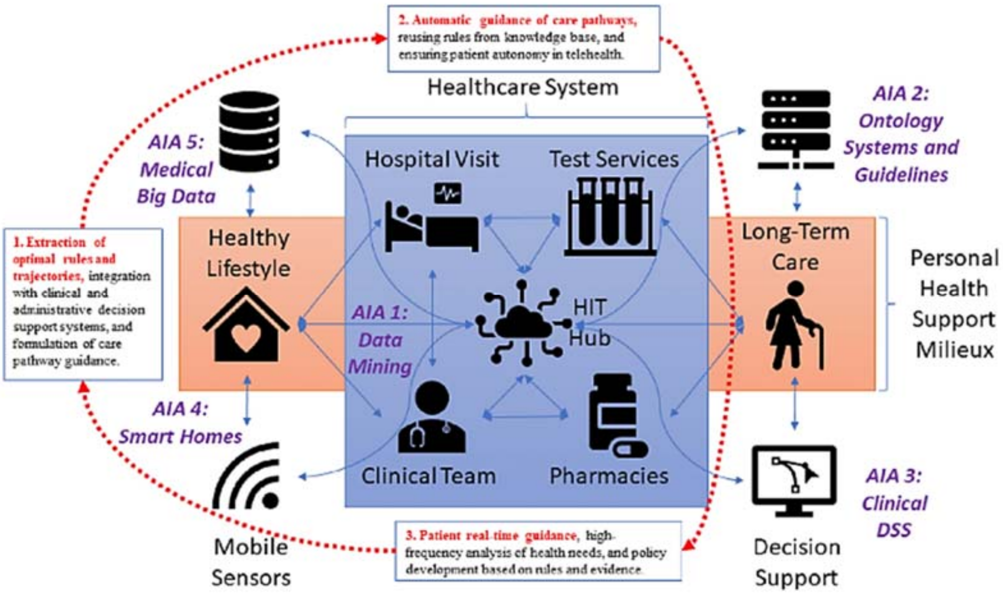
2. Automatic guidance of care pathways, reusing rules from knowledge base, and ensuring patient autonomy in telehealth.
Healthcare System
AIA 5: Medical Big Data
AIA 2: Ontology Systems and Guidelines
Hospital Visit
Test Services
1. Extraction of optimal rules and trajectories, integration with clinical and administrative decision support systems, and formulation of care pathway guidance.
Healthy Lifestyle
AIA 1: Data Mining
HIT Hub
Long-Term Care
Personal Health Support Milieux
AIA 4: Smart Homes
Clinical Team
Pharmacies
AIA 3: Clinical DSS
Mobile Sensors
3. Patient real-time guidance, high-frequency analysis of health needs, and policy development based on rules and evidence.
Decision Support

Fig. 3 Healthcare application of AI and analytics

### *B. Data Protection in AI-Driven Healthcare Systems*

AI-powered healthcare solutions involve a broad range of use cases that use AI algorithms to improve different healthcare aspects to enhance patient outcomes. AI-enabled healthcare systems leverage the power of AI to analyze a large amount of healthcare information, generate valuable insights, and help medical stakeholders make informed decisions [15]. The primary elements of AI-driven healthcare systems can be explained in the overview below:

- Information gathering: AI-driven healthcare solutions rely on the gathering of diverse medical information such as medical imaging data, EHRs, wearable device data, sensor-derived data, genomic data, and patient-generated information. Healthcare data from diverse sources is comprehensive and contains information regarding patients' health conditions, monitoring information, and their medical history.
- Data analysis and Decision-making: AI-powered algorithms are leveraged in the analysis and interpretation of healthcare information, allowing enhanced analytics and hence informed decision-making. ML-based methods, like supervised, unsupervised, and reinforced learning may be used to spot patterns, identify anomalies, forecast outcomes, and offer individualized recommendations to medical practitioners.
- Medical Diagnostics and Imaging: Lately, AI-powered healthcare solutions are making a great impact on medical imaging analysis. Healthcare AI is used to analyze medical images, like CT scans, MRIs, and even X-rays, to help detect and diagnose illnesses and health conditions such as cancers, cardiovascular diseases, and neurological conditions [16]. Also, AI algorithms are leveraged in automated image recognition and segmentation systems to enhance the efficiency of disease diagnosis.
- Personalized Treatment and Planning: AI-based algorithms help to plan treatment through patient data analysis, healthcare literature, and clinical guides. They provide tailored treatment recommendations, drug interaction identification, and adverse reactions. AI-powered healthcare systems support precision medicine where genomic data is used to customize treatment plans depending on a person's genetic profile.
- Remote Patient Surveillance: AI-powered healthcare solutions assist medical professionals in monitoring patients remotely, allowing them to extract vital information regarding disease symptoms and treatment

adherence. These systems help analyze real-time patient data and notify healthcare providers of any anomaly or emergency. These solutions are particularly important for the management of chronic conditions and postoperative care.

- Virtual Assistant and Medical Bots: AI-enabled virtual assistant solutions and medical chatbots play critical roles in healthcare such as providing tailored health data to patients, responding to questions, and helping in planning appointments [17]. AI-powered conversational tools leverage NLP capability to comprehend and react to patients' queries, thus enhancing access to healthcare data and minimizing administrative burden.
- Clinical and Drug Research: AI-powered healthcare solutions immensely contribute to the acceleration of drug discovery and production methods. AI is used to analyze vast amounts of datasets to identify significant drug targets, project drug efficiency, and optimize the design process for clinical trials. This AI use case in medicine promises more cost-effective and efficacious drug production.
- Resource Management and Healthcare Operations: AI-powered healthcare systems help optimize medical processes by forecasting the flow of patients, enhancing consultation and treatment schedules, and optimizing the allocation of resources. ML-based and predictive analytics methods assist healthcare providers in simplifying workflows, shortening waiting times, and improving operational efficacy.

## II. Background

### A. Artificial Intelligence and Data Privacy

Data privacy is critically important in healthcare and most cases, users want to protect sensitive, valuable information before deploying or building AI-powered systems. Let us look at medical research or an AI model trained for healthcare specialists from EHRs. If the owner of the data and the computation party are different, then the private information should be sent to the calculation party via secure media. However, most probably it would need to be stored on the computer server and in its original form, implying it should not be changed or encrypted. This way, such sensitive information would be susceptible to internal and external attacks, posing security risks like manipulation, theft, or damage. Therefore, data privacy involves numerous elements including features, exact values, and membership of the information.

In the ML and big data context, data privacy implies protecting data against adversarial assaults with a primary objective of inferring sensitive, valuable information from a victim, leading to inadvertent data leakage. With the increasing number of businesses and industries adopting big data analytics, big data has exceedingly revolutionized the digital realm and its impacts get more and more pervasive. In the modern digital age, our ability to control/manage how we store, share, or update our information is critically important in terms of preserving our privacy. Over time, with the resurgence of robust web-enabled data mining technologies, data privacy has gradually become a social concern. Data privacy and autonomy over personal data have become increasingly important due to the explosion in big data and the AI era; the vital elements of privacy preservation and AI add to risks associated with personal privacy.

### B. Development of Progressive Healthcare AI

Healthcare AI has tremendously grown over the past few years. AI-driven solutions are now used to conduct critical medical procedures like medical imaging, support decision-making and virtual assistant tasks, medical bots, and drug R&D [18]. In the past decade, several solutions developed by healthcare AI have been accredited by healthcare regulators and relevant authorities. These technologies include solutions used for orthopedics, cardiovascular, respiratory, and ophthalmology. Specifically, market sectors that develop and deploy best-in-class healthcare solutions, like AI-driven medical imaging and drug research have manifested tremendous growth.

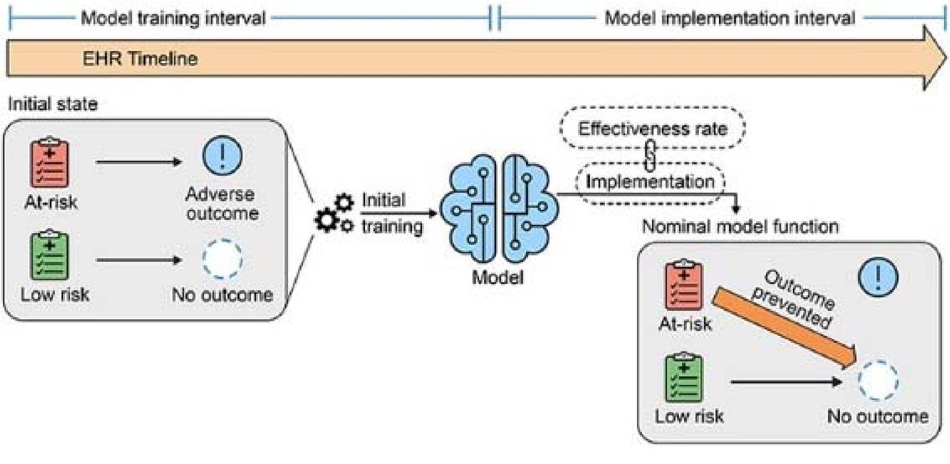

Fig. 4 Training AI-algorithms used in healthcare with patient data

The World Health Organization (WHO) affirms that AI has "immense capacity to strengthen the healthcare delivery [19] Today, AI solutions are used to support various medical undertakings such as disease diagnosis, imaging, drug development, and individualized treatment. In public health and epidemiological affiliated areas, AI assists in the deployment of interventions like infection monitoring, outbreak response, and healthcare systems management [20]. Nevertheless, the use of AI presents challenges and risks associated with healthcare ethics and human rights. For example, AI applications threaten people's privacy, impact the autonomy of decision-making and dignity, and are associated with algorithmic biases, among others.

There have been concerns about the protection of personal privacy caused by the breach of privacy rights with the deployment of AI in healthcare systems. This failure to protect patient privacy may result in adverse repercussions, like occupation discrimination and high cost of healthcare provision [21]. Previously, physical documents were used to record and store healthcare data, where privacy protection largely informed concealing patients; identity, and preserving their confidentiality among medical employees within healthcare organizations (HCOs). Today, digital solutions are increasingly used to record and store patient data, where large volumes of data are collected and shared among different medical stakeholders for various purposes. Since healthcare AI is founded on the amalgamation and consumption of patient data, privacy protection concerns have become increasingly sophisticated in a time when data sharing is never so profitable and convenient.

Historically, however, there has never been a steady stipulation of privacy rights. Generally, privacy laws/policies have been vague, fragmented, and even insufficiently enforced. Personal information has frequently been infringed and data breaches in healthcare have damaged public confidence regarding data handling. Such incidents, accompanied by social political space where people's right to privacy is subservient to social goals, usually discourage the sustainable development of healthcare AI.

### *C. Modern Healthcare AI Protects Patient Data Privacy*

A team of researchers from the Technical University of Munich (TUM) developed a model technology that protects sensitive patient information while training healthcare AI algorithms [22]. Their invention has since been deployed in an algorithm that detects pneumonia in children using X-ray images. The scientists discovered that their novel privacy protection technology manifested relatively comparable or greater accuracy in diagnosing a variety of pneumonia in young ones than traditional algorithms [22].

Clinicians can use AI algorithms to diagnose diseases and health conditions like malignant cells (cancers) and sepsis. The efficiency of the AI algorithms fundamentally depends on the amount and quality of information that is employed for the training and healthcare data is usually shared amongst HCOs to optimize the pool of data. While data protection measures such as pseudonymization and anonymization are often used to secure/protect the data, scientists argue that these data protection measures are inadequate. This challenge was addressed by an interdisciplinary team of researchers drawn from TUM, the UK-based Imperial College London, and a non-profit organization firm OpenMined devised a novel combination of AI-driven diagnostic procedures to conduct radiological image information that protects data privacy.

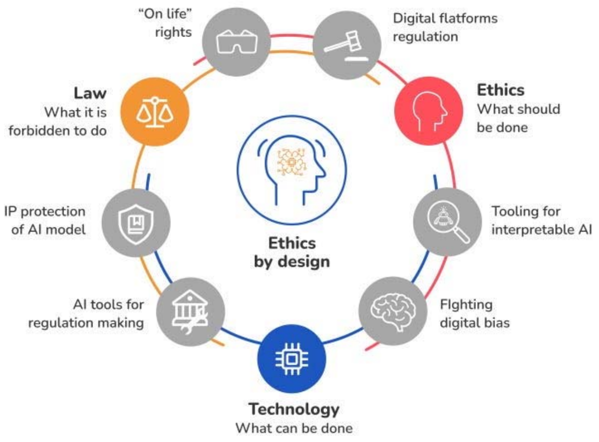

Fig. 5 Ethical and legal aspects considered in the protection of healthcare AI applications

One notable technique to secure patients' data is to keep it at the collection site instead of sharing it with other HCOs. Nevertheless, most HCOs share patient information by sending duplicates of databases to HCOs that deal with the training of AI algorithms. Also, to ensure the identity of the institution where the training of the AI algorithms was performed anonymously, the trainers follow special techniques such as the aggregation technique [22]. Here, the training team merges the AI algorithms in encrypted format and later decrypts them after training has taken place. Also, to avoid the personal information of the patients from filtration leading to divulgence of their identities, researchers training the AI algorithms may use a third method to ensure that only the statistical correlations are extracted from the information, but not what a person contributes.

## III. Materials and Method

### *A. Research Information*

In this qualitative review, an empirical study of the current development in healthcare AI privacy protection was done. Corresponding research conducted by various researchers and organizations was studied. Concerning the preservation and breach of healthcare data, official reports from relevant government authorities were also analyzed. Moreover, the examination included news reports involving the leakage of personal data. Besides, information about lawsuits and criminal cases decided in the court of law was also analyzed and data were collected. Concerning data on the preservation of patient privacy across the globe, the official sites of various governments were reviewed to collect relevant information on this issue. Finally, to gather detailed information on privacy protection policies, laws, and regulations across the globe, the study exercised various professional legal databases employing keywords such as "data privacy", "personal data", "informed consent," "Healthcare AI," "AI privacy," and "cross-border information flow" among others.

### *B. Research Methods*

An all-inclusive literature survey of global development in data privacy preservation regulations for medical data leveraged to train AI algorithms and systems was conducted. An empirical study of cross-border privacy protection regulations and controls, law enforcement measures, and legal implications formed the foundation of this study. Moreover, a study into how different regulatory authorities respond to cases involving personal data was conducted.

In addition, the study compared various data privacy protection measures across the world. Relevant data privacy preservation regulations from different countries were gathered from official and present government sources, tabulated in a rubric for extensive comparison and analyzed. The differences between the laws were identified and further research into official descriptions for the formulation of these regulations from respective governments and different legal sources was also conducted. Comparing the various legal provisions regarding data privacy protection underscored gaps in some of the current privacy protection laws.

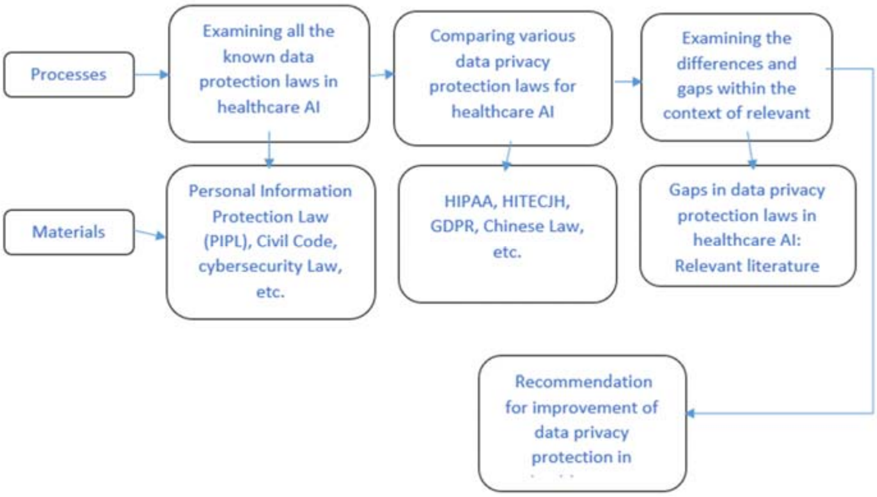
Processes
Examining all the known data protection laws in healthcare AI
Comparing various data privacy protection laws for healthcare AI
Examining the differences and gaps within the context of relevant
Materials
Personal Information Protection Law (PIPL), Civil Code, cybersecurity Law, etc.
HIPAA, HITECJH, GDPR, Chinese Law, etc.
Gaps in data privacy protection laws in healthcare AI: Relevant literature
Recommendation for improvement of data privacy protection in

Fig. 6 Processes and materials employed in this project

## IV. Results

### *A. Cradle, Regulatory Status and Legal Practice*

The belief that advanced computer programs can simulate human intelligence was initially suggested in the 1950s by Alan Turing when he published his seminal paper titled, "Computing Machinery and Intelligence" exploring machine intelligence and that introduced concepts like the "Turing Test." Advanced healthcare AI applications came into the limelight in the 1970s with the birth of backward chaining expert technology employing goal-directed control programs referred to as MYCIN. The MYCIN system used AI algorithms to identify infections related to blood clotting conditions, though its application in medicine did not mature due to ethical and legal issues associated with the application of computers in healthcare. A more advanced healthcare AI system was unveiled by Watson in 2007 which used AI to develop a question-answering system referred to as DeepQA. The healthcare AI technology, now known as Watson Health or simply Merative, is used to analyze vast amounts of healthcare data to offer tailored and evidence-based health recommendations and helps medical professionals to make informed decisions [23]. Also, other AI-powered healthcare solutions like Microsoft's Bio Model Analyzer and Google's DeepMind play critical roles in improving clinical operations and enhancing patient care [24].

Since the start of 2021, the world has made tremendous advancements in the field of healthcare AI. Also, the healthcare AI market size has exceedingly increased over the past two decades with clinical decision support systems (CDSS) registering the largest growth rate. Simultaneously, the rapid development and deployment of AI in healthcare technology has resulted in an escalated risk for healthcare data breaches. For instance, since medical imaging data contain huge volumes of private patient data without adequate desensitization, a large amount of non-desensitized medical imaging data is exported. Breaches in private patient information may result in a violation of their right to privacy, thus it is recommended to generate fair and operational data security and privacy protection policies and measures.

In terms of legal implication and court cases, for instance, the Supreme People's Court of China realized in its yearly work report that the country's courts had handled around 4098 lawsuits related to numerous criminal offenses against citizens' private data in 2021, which accounted to a 60.2% year-on-year increase. The crimes were related to the stealing and sale of identity cards, courier lists, address books, as well as WeChat accounts [25]. The intermediate People's Court in Hangzhou handled a high-profile data privacy battle referred to as the "China's First Facial Recognition Case", which was critical for the regulation of personal data and data privacy in the country, as the outcome emphasized the need for healthcare data handlers and healthcare professionals to engage in lawful gathering and consumption of personal information.

### B. Data Privacy Protection Frameworks

1. Acts and Policies

- EU's General Data Protection Regulation (GDPR): GDPR is a European Union data security law that came into effect in 2018. Though only applies within the EU's jurisdiction, its norms may be used as a guide to any country beyond Europe. Essentially, GDPR promotes the development of digital technologies that consider the privacy of data owners.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA): The HIPAA act was initiated in 1996 as a federal law. This act formulates the standards for processing and handling patients' health data and prohibits the divulgence of the information without their willingness or knowledge.
- Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS): This act aims at formulating Autonomous and Intelligent Systems policies and standards, to guarantee their security, adherence to ethical principles, and benefit to society. The act also emphasizes the stimulation of public participation when creating ethical frameworks to bolster public comprehension of ethical issues associated with technology.
- Digital Personal Data Protection Bill, 2023: Introduced in 2019, this bill underwent public participation and was ultimately passed in 2023. This act regulates all electronic personal information and dictates that such type of information can only be consumed after informed consent of the data owner, but provides exceptional instances when that data may be used based on authority and purpose of consumption. Also, the act obligates the fiduciaries of the data to preserve its accuracy, keep it secure, and delete it once its objective has been met. Since this is an Indian act, the act prohibits the transfer of personal information outside of the country, apart from specific countries mentioned by the Indian government. The act stipulates the amount of fine a person or business must pay if found guilty of breaching data privacy laws or failing to configure adequate data security measures to bar data breaches.

2. AI Models-Based Data Privacy Protection Methods

- Federated Learning Technique: Since the transfer of sensitive data may lead to data leaks and is especially chaotic in the event the transfer is to be done across the border, trials have been executed at the transferring networks, instead of the data itself. A federated learning technique encompasses a distributed learning model where numerous clients work in conjunction to collectively develop a secure model while preserving the privacy of their input [26]. Using the federated learning model, learning is conducted separately, every time with a different data set, and the model that results from the training draws knowledge from diverse sets of data.
- Cryptographic Techniques: As the name suggests, this data privacy preservation technique allows data processors to encrypt the data before putting it into training and testing. Cryptographic data privacy protection methods are broadly classified as Homomorphic Encryption (HE) or Secure Multi-Party Computation (SMPC).
- Differential Privacy Technique: This is a mathematical technique that adds the aspect of randomness and/or noise to valuable data in the bid to hide the contribution made by each participant.
- Hybrid Privacy-preserving Method: This is a hybrid approach that combines all the aforementioned data privacy protection techniques to guarantee data privacy and security in the healthcare domain [27].

## V. Discussion and Conclusion

Whereas AI technology widens pathways for development in healthcare and enhancement of patient care outcomes, there are several data security concerns related to patient privacy that should be addressed, particularly regulation of the processing and handling of patient healthcare data before, during, as well as after using it for training AI algorithms. The formulation of a legal protection technique/system should balance technological advancement and data privacy protection. Healthcare providers should be barred from breaching patient's rights to privacy in their pursuit of boundless technologies to gain a competitive edge and satisfy their stakeholders. Also, technological development and profits should not be achieved at the expense of other people's privacy, as the objective of any technological advancement is to improve the living standards of humankind.

Healthcare organizations and relevant processors of patient data must implement data security and bolster insider controls and handling of valuable, sensitive personal data based on legal provisions. To construct a robust legal framework to protect data privacy – which is a critical gap in many AI-specific Laws – authorities should promulgate special regulations in concert with popular data security domain-specific laws such as Personal Information Protection Law (PIPL) to create a dual regulation structure, that is, "basic law + special law that defines healthcare and health data processing policies. Within the framework, different actions need to be taken: (1) consolidate concepts associated with health data in numerous legal documents; (2) classify information and formulate several rules for special data types; (3) enhance the interactive nature of consent via digital informed and dynamic consent to improve the efficiency of "informed consent;" and (4) develop a robust accountability mechanism to guarantee the violation of rights to privacy in healthcare AI is regulated and mitigated.

Further, to develop a global network for information governance in the medicine domain and broaden pathways for data sharing, countries and healthcare organizations should actively engage in developing a global legislative infrastructure for healthcare data governance. Regarding the gaps and uncertainties in information governance policies among varied countries, it is important to bolster information protection and foster cross-border information flow through global soft law. Lastly, healthcare providers should consider WHO guidance on healthcare AI governance to promote sturdy data privacy.

## References

[1] Jumper J., Evans R., Pritzel A., Green T., Figurnov M., Ronneberger O., Tunyasuvunakool K., Bates R., Žídek A., Potapenko A., Highly accurate protein structure prediction with AlphaFold Nature, 2021 596 (7873) pp. 583-589

[2] Milana C., Ashta A. Artificial intelligence techniques in finance and financial markets: A survey of the literature. 2021. 30 (3) pp. 189-209

[3] Statista. Artificial intelligence (AI) in healthcare market size worldwide from 2021 to 2030. 2024. Available at: https://www.statista.com/statistics/1334826/ai-in-healthcare-market-size-worldwide/#:~:text=It%20was%20forecast%20that%20the

[4] Vemuri, Naveen. AI-Optimized DevOps for Streamlined Cloud CI/CD. International Journal of Innovative Science and Research Technology: 2024. 9.7.10.5281/zenodo.10673085.

[5] National Intelligence Council. Global Trends 2040: A More Contested World, 2021. COSIMO REPORTS. 9781646794973, 1646794974

[6] Hutan Ashrafian, Niklas Lidströmer. Artificial Intelligence in Medicine. 2022. Springer International Publishing.

[7] Halling-Brown M. D., Warren L. M., Ward D., Lewis E., Mackenzie A., Wallis M. G., et al. OPTIMAM Mammography Image Database: A Large-Scale Resource of Mammography Images and Clinical Data. Radiol Artif Intell. 2021; 3:e200103.

[8] Murdoch B. Privacy and artificial intelligence: Challenges for protecting health information in a new era. BMC Med Ethics. 2021; 22:122.

[9] Moshawrab M., Adda M., Bouzouane A., Ibrahim H., Raad A. Reviewing federated machine learning and its use in diseases prediction. Sensors (Basel) 2023; 23:2112.

[10] Sailakshmi V. Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud; 2021.

[11] Kayoe, S., & Godwin, O. Examining the effects of worldwide developments, such as the emergence of online learning and the growing emphasis on global cooperation: 2023.

[12] Nyathani, Ramesh. Integration of Industry 4.0 and Human Resources: Evolving Human Capital Management and Employee Experience through Digital Innovations: 2022.

[13] Kayoe, S., & Godwin, O. Examining the effects of worldwide developments, such as the emergence of online learning and the growing emphasis on global cooperation: 2023.

[14] Bernd Carsten Stahl. Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies. 2021. Springer International Publishing

[15] Kalla, Dinesh & Samaah, Fnu & Kuraku, Sivaraju & Smith, Nathan. Phishing Detection Implementation Using Databricks and Artificial Intelligence. SSRN Electronic Journal. 2023. 185. 10.2139/ssrn.4452780.

[16] Chowdhury D., Dey A., Garai R., Adhikary S., Dwivedi A.D., Ghosh U., Alnumay W.S. Decrypt: A 3DES inspired optimised cryptographic algorithm J. Ambient Intell. Humaniz. Comput. (2022), pp. 1-11

[17] Paul J., Annamalai M. S. M. S., Ming W., Al Badawi A., Veeravalli B., Aung K.M.M. Privacy-preserving collective learning with homomorphic encryption IEEE Access, 9 (2021), pp. 132084-132096

[18] Rasheed K., Qayyum A., Ghaly M., Al-Fuqaha A., Razi A., Qadir J. Explainable, trustworthy, and ethical machine learning for healthcare: A survey Comput. Biol. Med. (2022), Article 106043

[19] World Health Organization Ethics and Governance of Artificial Intelligence for Health. (Accessed on 24 February 2024). Available online: https://www.who.int/publications/i/item/9789240029200

[20] Zeng D., Cao Z., Neill D. B. (2021). Artificial Intelligence in Medicine: Artificial intelligence–enabled public health surveillance, From local detection to global epidemic monitoring and control; Academic Press; Cambridge, MA, USA: pp. 437–453.

[21] Akgün M., Pfeifer N., Kohlbacher O. Efficient privacy-preserving whole genome variant queries Bioinformatics (2022)

[22] Caroline Brogan. New AI technology protects privacy in healthcare settings. (2021). Available at: https://www.imperial.ac.uk/news/222093/new-ai-technology-protects-privacy-healthcare/

[23] IBM. IMB Watson Health. (Accessed on 27 February 2024). Available online: https://www.ibm.com/watson-health.

[24] Bass D. Microsoft Develops AI to Help Cancer Doctors Find the Right Treatments. (Accessed on 27 February 2024). Available online: https://www.bloomberg.com/news/articles/2016-09-20/microsoft-develops-ai-to-help-cancer-doctors-find-the-right-treatments

[25] Work Report of the Supreme People’s Court. At the Fifth Session of the Thirteenth National People’s Congress on 8 March 2022. (Accessed on 28 February 2024); Available online: https://www.court.gov.cn/zixun-xiangqing-349601.html

[26] Ali A., Ilahi I., Qayyum A., Mohammed I., Al-Fuqaha A., Qadir J. Incentive-driven federated learning and associated security challenges: A systematic review (2021)

[27] Torkzadehmahani R., Nasirigerdeh R., Blumenthal D. B., Kacprowski T., List M., Matschinske J., Privacy-Preserving artificial intelligence techniques in Biomedicine. Methods Inf Med. (2022). 61:e12–27.