

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN HEALTHCARE: DEVELOPING PRIVACY-PRESERVING FRAMEWORKS

Chidiebere Udeokechukwu¹, Ogbodo Chijioke^{2*}, Ugochukwu Echendu³, Annastecia
Chinweikpe Oguanya⁴

UNIVERSITY OF NIGERIA NSUKKA

*Correspondence: Ogbodo Chijioke

Contact: ogbodochijiokesunday2000@gmail.com

*The authors declare
that no funding was
received for this work.*



Received: 17-July-2025

Revised: 25-July-2025

Accepted: 01-August-2025

Published: 05-August-2025

Copyright © 2025, Authors retain copyright. Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/4.0/> (CC BY 4.0 deed)

This article is published by **MSI Publishers** in **MSI Journal of Multidisciplinary Research (MSIJMR)**

ISSN 3049-0669 (Online)

Volume: 2, Issue: 8 (August-2025)

ABSTRACT: This paper investigates the groundbreaking capabilities of Artificial Intelligence (AI) within healthcare, concurrently addressing critical patient data privacy concerns. It methodically reviews scholarly articles on AI applications, data protection techniques, and relevant legal frameworks. The study introduces a novel AI framework, Safe Sync-Aegis AI (S²AI), conceived by integrating the strengths of diverse privacy-preserving methods such as Differential Privacy (DP), Federated Learning (FL), Homomorphic Encryption (HE), Blockchain Technology, and Secure Multi-Party Computation (SMPC). While acknowledging AI's profound potential to revolutionize healthcare, the research identifies considerable privacy risks associated with sensitive patient information. A core finding emphasizes the necessity of a comprehensive strategy that blends robust privacy techniques, stringent data protection protocols, and ethical considerations for responsible AI adoption. Special attention is given to the Nigerian context, highlighting the urgent need for substantial legislative and regulatory reforms to accommodate AI's complexities. The proposed S²AI framework aims to deliver superior privacy, scalability, security, and regulatory adherence, though its implementation may present challenges in complexity and

processing efficiency. The paper concludes by stressing the vital importance of balancing AI's transformative power with stringent privacy safeguards and ethical guidelines to foster a trustworthy and equitable healthcare future.

I-INTRODUCTION

The convergence of computer science and medicine has led to groundbreaking technological advancements in healthcare (Kulikowski, 2019). Starting in the 1950s, researchers explored the possibility of machines mimicking human cognition (Vation Ventures, n.d.). The practical application of AI in medicine began in the 1970s (Miller et al., 1982). In 1971, INTERNIST-1, the first artificial medical consulting system, was developed. This system utilized a search algorithm to diagnose illnesses based on patient symptoms. It was a significant advancement in AI for clinical research as it had the potential to lessen the diagnostic workload on healthcare providers and enabled physicians to verify their differential diagnoses.

The clear potential of AI in medicine led to the National Institutes of Health funding the inaugural AI in Medicine conference at Rutgers University (Kulikowski, 2019). The growth of AI in medicine was partly inspired by interdisciplinary gatherings where researchers traded ideas and systems. One such system that emerged from this collaboration was MYCIN, which was designed to aid physicians select appropriate antibiotics for infectious diseases based on specific input criteria (Shortliffe, 1977).

Another key development occurred in the 1980s at the University of Massachusetts with the creation of DXplain, a program intended to help clinicians in making medical diagnoses (The Laboratory of Computer Science n.d.). Similar to INTERNIST-1, DXplain enabled clinicians to key in symptoms and obtain potential diagnoses in return. But it also offered a wider range of possible diagnoses and served as an early resource for physicians seeking current medical information (Hirani et al., 2024).

In more recent times, advanced technologies have emerged that can analyze large datasets, identify patterns, and offer insights that enhance human decision-making (Mintz & Brodie, 2019). IBM's Watson, a prominent example, uses sophisticated language processing to gather information from various sources (Bakkar et al.,

2018). This ability has significant implications for healthcare, allowing for the analysis of complex medical data to improve diagnosis, treatment, and research efforts.

Considering the immense promise of these technologies for healthcare, safeguarding patient privacy becomes paramount. Incorporating data-driven solutions into medical practice generates crucial concerns regarding adherence to data security laws, like the Health Insurance Portability and Accountability Act (HIPAA). For ethical and responsible implementation of these advancements, a reliable structure emphasizing privacy-preserving techniques and strict data protection protocols is unavoidably germane.

This precursor establishes the groundwork for a thorough investigation into the integration of cutting-edge technologies within healthcare, with a focus on protecting patient confidentiality and maintaining adherence to relevant legal frameworks.

Potential benefits of AI application in healthcare

The field of healthcare is experiencing a period of substantial change, fueled by innovative technologies reshaping medical practices and tackling critical worldwide health issues (Jumper et al., 2021). For example, recent progress in areas like protein structure prediction has provided solutions to longstanding biological and medical puzzles (Jumper et al., 2021). In a similar vein, progress in simulated clinical trials now permits pharmaceutical firms to assess drug effectiveness across broader virtual populations, potentially yielding more efficacious therapies (Ekins et al., 2020).

The growing accessibility of extensive data repositories, coupled with technological progress and advanced algorithmic methods, has spurred the rise of data-centric methodologies in healthcare (Bohr & Memarzadeh, 2020). Notably, deep learning strategies have demonstrated considerable efficacy in areas such as medical image classification and the analysis of complex, multi-faceted datasets (Kihara et al., 2019). These innovative approaches hold the potential to revolutionize how we diagnose, treat, and prevent diseases (An et al., 2023).

Blending machine learning algorithms with substantial datasets, encompassing genetic data and electronic health records, has heralded individualized medical strategies (Bohr & Memarzadeh, 2020). Mobile health apps, which collate and analyze patient data, have also shown potential in delivering customized treatment recommendations (An et al., 2023). Moreover, leveraging machine learning to analyze genetic information and biomarkers has facilitated the prediction of treatment outcomes and the development of tailored therapies (Love-Koh, 2018).

According to Kirch and Petelle (2017), healthcare organizations are striving to adapt to these rapid technological changes and fulfill increasing patient demands for enhanced services and results; and Marr (2018) posits that priority areas of development encompass streamlining administrative processes, enhancing image analysis techniques, implementing robotic surgical procedures, utilizing virtual support systems, and improving clinical decision-making tools. Furthermore, data-driven methods have also demonstrated potential in forecasting disease progression and outcomes for conditions like acute kidney injury and age-related macular degeneration (Arcadu et al., 2019).

The use of machine learning in healthcare has become increasingly prevalent because of its capacity to process sophisticated data and generate insights that guide medical decisions (Garg & Mago, 2021). Yan et al. (2016), along with several other studies reecho the fact that contemporary research has earmarked the efficacy of these methods in tasks such as identifying anatomical structures in medical images, classifying interstitial lung diseases (Anthimopoulos et al., 2016), reconstructing medical images (Schlemper et al., 2017), and segmenting brain tumors (Mehta & Majumdar, 2017).

II—LITERATURE REVIEW

Haleem *et al.* (2019) noted that the incorporation of trailblazing technologies has enhanced healthcare for the better; encouraging advancements in both patient care and health outcomes. Sophisticated computer systems are currently used for a variety of purposes, including hospital administration, diagnostics, and treatment planning (Haleem et al., 2019). It is also worth noting that computer-assisted medical picture

analysis, automated pharmaceutical production, electrocardiogram and blood test analysis are becoming more efficient with the help of superior hospital computer systems (Los Angeles Pacific University, 2023; Park et al., 2020).

Recent research establishes the prospects of leading-edge technologies in healthcare, indicating the potential for more efficient diagnostic precision, precise treatment strategies, and optimised patient care (Alowais et al., 2023; Roy, 2022). To buttress this, Park et al. (2020) highlights that intricate image processing technologies allow for easy and quick analysis of medical visuals, accelerating diagnosis. Notably, Natural Language Processing (NLP) techniques convert unstructured material into usable formats, making it easier to analyse patient health information and medical history.

The issue of sensitive patient data with the emergence of advanced technologies in healthcare raises important concerns, including data breaches and potential exploitation (Roy, 2022). To address these problems, solid data protection systems are critical for striking a balance between patient confidentiality and innovations in health technologies (Tom et al., 2020).

The integrity of telehealth depends incredibly on strong data security and confidentiality measures (Hall & MacDrew, 2014). In the same vein, Roy (2022) points out that personalized medicine approaches, which are hinged on individualized patient data, also pose challenges related to data vulnerabilities and potential biases in data utilization, highlighting the need for strict data management practices (Roy, 2022).

The harmonious merging of leading-edge technologies in healthcare, although innovative, demands a progressive strategy to protect patient confidentiality. In light of this, it becomes crucial to stress again that establishing robust data protection measures is important to counter unauthorized data breaches and guarantee the safe handling of sensitive patient data, thereby upholding ethical standards in healthcare (Williamson & Prybutok, 2024).

A review of recent works by Nigerian authors reveal the potential of AI to enhance national security and the aftermath problem of regulating its deep impact on data privacy.

One of the works argues that AI is now an unavoidably necessary and authorized instrument for addressing Nigeria's serious security concerns, such as terrorism, cybercrime, and banditry (Okeke et al., 2024). This viewpoint advocates for utilizing artificial intelligence in cases such as predictive policing and real-time monitoring to strengthen state security objectives. However, another body of research warns that these artificial intelligence applications constitute serious data privacy concerns that Nigeria's regulatory frameworks are not yet prepared to address (Adedeji, 2025; Anagbogu, 2025; Salami & Nwankwo, 2024).

These researchers contend that there is a direct conflict between AI and data privacy. The "black-box" architecture of AI systems, which is the absence of openness on the methodology used by machine learning models, especially deep learning systems, to get their results, jeopardises transparency and accountability—a serious shortcoming of governance identified in several studies—recurs frequently in this conversation (Adedeji, 2025; Salami & Nwankwo, 2024).

III—LEGAL AND ETHICAL CONSIDERATIONS

Governments have implemented legislation to safeguard individual privacy, with countries such as Australia, Canada, the UK, and the US enacting relevant laws (Khalid et al., 2023). However, the actual impact of these laws in protecting privacy remains uncertain. The United States Congress enacted the HIPAA in 1996 to protect sensitive healthcare information, while the European Union's General Data Protection Regulation (GDPR) introduced in 2018 expanded on the earlier Data Protection Directive of 2012, which itself built upon the 1995 directive (Bennett et al., 2012; Maxenier, 1995). The landmark Belmont Report in the United States laid the groundwork for essential ethical principles in research, emphasizing the importance of respecting an individual's autonomy, promoting well-being, avoiding harm, and upholding fairness and justice (National Commission for the Protection of

Human Subjects of Biomedical and Behavioral Research, 1979; Abramoff, Tobey, & Char, 2020).

The GDPR empowers EU residents with the right to data erasure, establishing a robust framework for data protection within the EU and European Economic Area (EEA) (Politou et al., 2018). Nevertheless, AI-driven healthcare solutions pose significant threats to patient confidentiality, particularly concerning the handling and management of sensitive medical information. A prominent illustration is the 2016 controversy surrounding the collaboration between Royal Free London NHS Foundation Trust and DeepMind, which raised concerns about unauthorized sharing of patient data (Murdoch, 2021). The growing involvement of private entities, such as Alphabet Inc., in collecting and utilizing sensitive patient data, combined with the increasing frequency of data breaches, worsens these concerns and highlights the imperative for enhanced data protection measures (Hirani et al., 2024).

As previously noted, there is a growing consensus amongst legal scholars that Nigeria's legal and policy frameworks are inadequately prepared for the complexities of AI (Adedeji, 2025; Anagbogu, 2025; Salami & Nwankwo, 2024). Despite the recent passage of the Nigeria Data Protection Act (NDPA), significant regulatory and enforcement gaps remain. Salami and Nwankwo (2024) argue that while instruments like the NDPA and the NDPR contain relevant principles, they are insufficient to address the tensions inherent in the AI data processing lifecycle. All three authors note that Nigeria's national AI policy is still in its nascent stage; hence, creating regulatory uncertainty and necessitating a more robust, principled approach to safeguard fundamental rights against the threats posed by AI systems.

The privacy risks identified stem from direct conflicts between how AI operates and core data protection principles. A recurring theme is the challenge of "algorithmic opacity"; the "black-box" nature of many AI models makes it difficult to scrutinize their logic, thereby undermining transparency and hindering a data subject's right to a meaningful explanation for automated decisions (Adedeji, 2025; Salami & Nwankwo, 2024).

Furthermore, the AI development stage presents several challenges, including establishing a lawful basis for collecting the massive volumes of data required for model training and adhering to the principle of data minimization. Salami and Nwankwo (2024) and Anagbogu (2025) emphasize that using biased or inaccurate training data can lead to discriminatory outcomes, violating the principle of data quality. Additionally, the ability of AI to generate unanticipated results encourages data repurposing, which conflicts with the purpose limitation principle that forbids processing data for reasons incompatible with its original collection purpose.

Obermeyer et al., (2019), Gerke et al., (2020) and Rashid et al., (2024) are of the view that the advancement of AI systems in healthcare requires a multifaceted approach to prevent biases that could perpetuate existing health inequities. Studies have demonstrated that racial biases can be embedded in healthcare algorithms, emphasizing the need for more refined definitions of care quality and data metrics. The rapid advancement of AI models, such as the transition from GPT-3 to GPT-4, highlights the importance of ensuring equitable access to these technologies to prevent exacerbating existing healthcare disparities (Achiam et al., 2024). To maintain ethical alignment, AI systems must undergo regular updates that incorporate local cultural and societal shifts (Rojas et al., 2022).

While AI has the potential to transform healthcare, it necessitates stringent privacy safeguards due to its reliance on sensitive data (Tilala et al., 2024). Decentralized data approaches, including Federated Learning (FL), Differential Privacy (DP), and Homomorphic Encryption, offer promising solutions for protecting individual privacy while enabling AI-driven insights (Bonawitz et al., 2021). Ultimately, singhal (2024) denotes a comprehensive strategy that integrates technical, governance, security, and ethical considerations is crucial for harnessing AI's benefits while upholding privacy and regulatory standards, thereby ensuring a trustworthy and equitable healthcare ecosystem.

The process of safeguarding patient data demands a nuanced strategy, which utilizes techniques such as data anonymization, de-identification, and differential privacy, in conjunction with privacy-enhancing technologies (PETs). These PETs facilitate data analysis without compromising confidentiality by sharing data directly

(Mosaiyebzadeh et al., 2023). Additionally, effective data governance necessitates exhaustive policies, stringent access controls, compliance with regulatory frameworks like HIPAA and GDPR, informed patient consent, transparency, data minimization, and regular security audits. Furthermore, reliable cyber security measures and ethical considerations, including accountability, bias mitigation, and patient data autonomy, are very important factors (Chon & Alexander, 2023).

Scheibner et al., (2020) notes that to comply with stringent data protection regulations, advanced de-identification techniques, such as k-anonymity and l-diversity, are germane, surpassing basic methods. Data minimization, a fundamental principle of GDPR, restricts collection of data to only necessary levels, with defined data retention policies. PETs play a vital role in supporting these compliance efforts (Walton, 2024). Transparency and control mechanisms, including informed consent and data breach notifications, are crucial for maintaining trust and ensuring regulatory compliance (Dhoriya, 2024).

The incorporation of AI in healthcare, encompassing diagnostics and patient care, holds vast promise, but its design and implementation must be anchored in stringent ethical and legal frameworks to safeguard sensitive patient information and ensure adherence to regulatory requirements (Alowais et al., 2023). Hence, innovative strategies, including FL, DP and Full Homomorphic Encryption (FHE), play a vital role in helping to attain AI-driven healthcare breakthroughs while preserving the confidentiality and integrity of patient data; and as a consequence there, upholding the trust and privacy of individuals (Radanliev et al., 2024).

IV—ANALYSIS OF PRIVACY-PRESERVING TECHNIQUES

Privacy-preserving analytics constitute a suite of methodologies designed to facilitate the analysis of sensitive data without exposing the underlying information's confidentiality. The main aim is to enable informative data analysis while protecting the privacy and secrecy of individuals and organizations, hence, upholding their trust and confidence (Ferrer, 2023). But reliability and credibility of telehealth solutions are heavily reliant on faithful implementation of robust security protocols and stringent data protection measures; because data breaches and compromised

technologies as highlighted by Hall & McGraw (2014) can undermine stakeholder confidence and trust. The ensuing paragraphs discuss several examples of Privacy preserving Techniques:

Differential Privacy (DP) Technique: According to Dyda et al. (2021), the differential privacy technique provides a strong safeguard against cyber related threats and data breaches by incorporating statistical noise into sensitive data. As a result of the noise addition, only aggregate patterns are disclosed in the course of shielding individual entities. This approach achieves anonymity by introducing a meticulously calibrated amount of random noise into the data or algorithmic outputs, rendering it statistically improbable for attackers to deduce sensitive information about specific individuals within the dataset (Williamson & Prybutok, 2024).

The versatility of DP facilitates its application across a broad spectrum of data types, including aggregated, de-identified, and synthetic data, thereby rendering it an essential tool for safeguarding data privacy in public health surveillance (Near et al., 2020). Moreover, DP can be effortlessly incorporated into various phases of machine learning workflows, ranging from data acquisition, processing to model development and inference (Tholoniati, 2023). The implementation of DP technology has profound implications for public health, enabling the secure sharing of detailed data, encompassing temporal, demographic and spatial information, while protecting confidentiality. Accordingly, this pioneering approach guarantees that algorithmic outputs do not jeopardize individual privacy, even when integrated with external data sources (Rao et al., 2018).

By harnessing the power of DP, researchers and health organizations can effectively shield sensitive information, tailor data sharing, and drive progress in public health research. An important instance of its successful implementation is the creation of a real-time COVID-19 data platform in Australia, showcasing its value in augmenting public health efforts (Dyda et al., 2021).

Federated Learning (FL) Technique: According to Martineau (2022) FL is a distributed machine learning paradigm that ensures collaborative development of AI models without needing the consolidation of data in a centralized repository. As

Bharati et al. (2022) elaborates, this approach allows multiple devices or organizations to jointly train a shared model, leveraging localized data insights whilst maintaining the confidentiality of individual data. Participants process data locally, sharing only incremental model adjustments with a central server, which then integrates the updates to refine the shared model via an iterative process that continues until the desired level of accuracy and reliability is attained.

FL offers significant potential for healthcare applications, empowering multiple stakeholders, such as hospitals, to collaboratively train AI models while enforcing stringent data protection measures (Wamat-Herresthal et al., 2021). Through the utilization of FL, healthcare data owners can ensure confidentiality of sensitive information by jettisoning the necessity for data sharing, thus reducing the risk of data breaches and unauthorized access (Sheller et al., 2020).

Full Homomorphic Encryption (FHE): Homomorphic encryption encompasses a radical advancement in cryptography. As a technique, it enables computations to be performed directly on encrypted data minus the need for decryption. According to Gaid & Salloum, (2021), this groundbreaking technique guarantees the secure delegation of machine learning tasks to external service providers and safeguards the confidentiality and integrity of sensitive data and models.

The integration of homomorphic encryption in the healthcare sector has profound consequences, encompassing secure data analysis, safeguarding genomic data, facilitating medical image analysis, and accelerating drug discovery. By leveraging this innovative technology, researchers can conduct intricate analyses on encrypted patient data without requiring access to the underlying raw data, thereby promoting collaborative research endeavors, enhancing healthcare outcomes, and preserving patient anonymity (Scheibner, Ienca, & Vayena, 2022).

Moreover, homomorphic encryption facilitates the processing and analysis of encrypted medical images without requiring decryption; hence there is room for confidential and secure diagnostic evaluations and treatment planning (Scheibner, Ienca, & Vayena, 2022).

Blockchain Approach: Blockchain technology provides a secure, decentralized infrastructure for healthcare data management, utilizing a distributed ledger system to guarantee the authenticity and tamper-proof nature of patient records. Blockchain effectively thwarts unauthorized access and potential data compromises, offering a reliable safeguard for sensitive medical information, and guaranteeing the confidentiality, integrity, and availability of patient data (Williamson & Prybutok, 2024).

The Blockchain technology can augment the interoperability of existing health records, providing a secure and trustworthy repository for medical data (Duca, Bacciu, & Marchetti, 2016). The convergence of blockchain and AI has the potential to transform the healthcare landscape by providing authenticated historical data, elevated privacy and security measures, enhanced compatibility, and optimized automation workflows (Khalid et al., 2023).

Secure Multiparty Computation (SMPC): SMPC is a specialized type of cryptography that facilitates collaborative data analysis by dispersing data across multiple entities. Each participant applies algorithms to their secure data, without accessing the data of other parties, thereby preserving confidentiality (Khalid et al., 2023). This technique ensures computation on distributed databases, allowing healthcare institutions to collectively analyze pandemic-related data without compromising information of sensitive nature.

Multiple hospitals are empowered at a go, to jointly train machine learning models on their combined datasets without sharing confidential patient data. Research underscores the potential of SMPC in mitigating healthcare fraud (Jangde et al., 2011). The simplicity and robust privacy protections of SMPC make it an attractive solution for collaborative data analysis and machine learning applications (Khalid et al., 2023). SMPC incentivizes collaborative machine learning among entities with complementary data, eliminating the need for data sharing (Hastings, 2021). For instance, healthcare institutions can jointly develop disease diagnosis models using their patient data, while maintaining patient anonymity and confidentiality.

Case Studies of successful utilization of data protection technologies.

A case study by Roy (2022) showcased the effective implementation of DP in a real-world public health setting through the COVID-19 Real-Time Information System for Preparedness and Epidemic Response (CRISPER) in Australia. Through the application of DP, the CRISPER initiative effectively protected individual privacy while facilitating the examination of aggregate trends in public health surveillance data. This enabled the disclosure of more granular information pertaining to temporal, spatial, and demographic factors without undermining privacy or confidentiality. The study attests to the vast potential of DP for widespread adoption in healthcare and other fields, offering a promising solution for individual privacy with data utility.

A 2013 research conducted a comprehensive security assessment of health information systems at three prominent Iranian medical facilities: Chamran, Al Zahra, and Amin Hospitals. Although the study did not concentrate on a specific data privacy technique, the paper employed a novel hybrid methodology, combining fuzzy AHP and TOPSIS approaches, to assess the overall security posture of the selected medical centers. This integrated framework facilitated the identification of critical security indicators, enabling the researchers to rank the centers based on their respective security levels. The study emphasized the importance of adopting a multifaceted security strategy, encompassing access control, network security, and data encryption measures. By analyzing these factors, the researchers identified areas of strength and vulnerability within each medical center's security framework, providing valuable insights for enhancing data protection and ensuring the confidentiality of patient information (Hajrahimi et al., 2013). This research demonstrated the efficacy of a comprehensive security assessment framework in identifying and mitigating potential risks to patient data, highlighting its significance in promoting data privacy and protection principles within healthcare settings.

A research paper by Dyda et al., (2021) discussed the use of differential privacy, a data protection technology, in the context of public health data sharing during the COVID-19 pandemic in Australia. The paper described a “worst-case adversary”

scenario where an individual with extensive knowledge about a community tried to identify a specific person's COVID-19 status from released data.

The study described the development of the COVID-19 Real-Time Information System for Preparedness and Epidemic Response (CRISPER) in Australia, which aimed to provide public health practitioners and researchers with access to detailed data on COVID-19 cases, testing, and contact tracing. CRISPER was programmed to utilize DP to protect confidential data whilst allowing for the release of aggregated statistics and visualizations.

The case study highlighted by the research demonstrated the feasibility of using DP to protect public health data whilst enabling data sharing for research and response efforts. DP allowed for the release of more granular data in terms of time, place, and person without compromising individual privacy.

Proposed AI framework for privacy protection and preservation: SAFE SYNC-AEGIS AI (S²AI)

This paper proposes S²AI, a novel privacy-preserving AI framework created by combining the strengths of the techniques discussed in this section—DP, FL, Fully Homomorphic Encryption (FHE), Blockchain, and SMPC. The meaning of the adopted name "Safe Sync-Aegis AI (S²AI)" is broken down as follows:

Safe: which denotes the AI system's primary focus on security, protection, and reliability.

Sync: which is short for "synchronize," highlighting the AI system's ability to harmonize and integrate with various data sources, systems, and stakeholders.

Aegis: derived from Greek mythology, Aegis refers to a shield or protective armor. In this context, Aegis represents the AI system's protective and defensive capabilities, safeguarding sensitive data and ensuring secure operations.

The acronym S²AI (pronounced "S2AI") is a concise and memorable representation of the full name. The superscript "2" stands for the synergy and synchronization aspects of the AI system. S²AI adopts the following integrated approaches:

Privacy at Data Entry (DP): Utilizing noise addition techniques to obscure individual data points from the outset. Hence, personal information remains confidential while still allowing for useful statistics.

Distributed Learning (FL): Employ a system where each organization trains a model on its own data, sharing only the improvements to the model, not the data itself. This approach keeps the data local while harnessing collective insights.

Secure Data Processing (Fully Homomorphic Encryption [FHE]): Implement advanced encryption allowing operations on data while data is still encrypted. This means that sensitive information can be analyzed or used in computations without ever being exposed in plain form.

Data Integrity and Traceability/Accountability (Blockchain): Utilizing a secure, decentralized ledger to record all actions taken on data or models. This ledger ensures that once information is logged, it cannot be altered, providing a clear audit trail.

Joint Analysis Without Sharing (SMPC): For collaborative projects, the framework will enable multiple parties to compute results together without revealing their data to each other, preserving privacy throughout the analysis.

How S²AI is designed to operate:

- **Data Gathering**: Information is gathered at each local site where DP is applied right away.
- **Local Analysis**: Each site processes its information, creating updates which are then encrypted before sharing.
- **Update Consolidation**: The encrypted updates are sent to a shared system where they are combined. The system uses encryption to ensure no one sees the actual data or interim results.
- **Model Improvement**: The combined updates are used to refine the model, with additional security for scenarios where multiple parties need to contribute without sharing their raw data.

- **Ledger for Governance:** All changes, permissions, and compliance activities are logged on the secure ledger, ensuring transparency and responsibility.
- **Application and Use:** The final models/insights are then leveraged locally, maintaining data privacy from commencement to conclusion.

Advantages

- **Increased Privacy:** Data stays secure and private at its source.
- **Scalability:** Programmed to grow with the number of participants and data volume.
- **Security:** Encrypted processes combined with a tamper-proof ledger.
- **Regulatory Compliance:** Built to meet strict data protection laws by default.

Challenges:

- **Complex implementation:** Combining these technologies can be intricate, potentially slowing down processes.
- **Lagging Performance:** Advanced encryption can be resource-heavy. Hence, the impacting the speed of applications will most likely be telling.

V—POLICY AND ETHICAL RECOMMENDATIONS

The confluence of AI and healthcare necessitates a well tailored strategy, considering the sensitive nature of medical information and the far-reaching ethical implications of its utilization (Richardson et al., 2021). As AI technologies continue to evolve, it becomes more pertinent to prioritize ethical considerations in order to ensure harmony with the foundational values of healthcare (Morley et al., 2019). The emergence of Large Language Models (LLMs) presents unprecedented regulatory hurdles (especially for jurisdictions like Nigeria), as existing frameworks struggle to accommodate their vast scale, capabilities, and adaptive characteristics. To address this challenge, new regulatory frameworks, ongoing surveillance, and validation across diverse populations are essential, complemented by the integration of ethical

principles such as equity, patient self-determination, and transparency to mitigate or ameliorate bias and healthcare inequities (Meskó & Topol, 2023).

The lack of transparency inherent in many AI algorithms, often described as “black boxes”, inspires apprehension and distrust, and hinders ethical accountability in healthcare decision-making processes (Williamson & Prybutok, 2024). In essence it becomes apparent that creating AI systems that balance technical expertise with interpretability is crucial for cultivating trust, informed decision-making, and responsible AI adoption. As healthcare professionals integrate AI into their practice, they must carefully consider the fundamental principles of medical ethics – patient autonomy, beneficence, nonmaleficence, and justice – to ensure that AI-driven decisions accord with these timeless ethical imperatives (Pasquale, 2020).

The global integration of AI in healthcare necessitates stringent data protection regulations, such as HIPAA and GDPR, to ensure the confidentiality and security of patient information (Alowais et al., 2023); therefore, fostering patient trust requires a transparent, accountable, and ethically grounded approach. To ensure the responsible deployment of AI in clinical settings, it becomes very imperative to implement robust data protection protocols, ethical frameworks, and informed consent procedures that prioritize patient autonomy and data sovereignty (Roy, 2022).

There is a need for a multi-faceted strategy that addresses both deployment of A.I and regulation. In Nigeria, scholars have identified several systemic barriers to progress, including pervasive corruption, significant infrastructural deficits, and a scarcity of skilled professionals, which hinder both the effective application of AI in several sectors including health and security, and the capacity of institutions to regulate it (Adedeji, 2025; Okeke et al., 2024). The proposed solutions universally call for the urgent establishment of a comprehensive legal and ethical framework that oversees AI use. This includes the adoption of a risk-based approach to regulation (Anagbogu, 2025; Salami & Nwankwo, 2024) and mandating proactive mechanisms like Privacy Impact Assessments (PIAs) and Privacy by Design (PbD) to embed data protection into the technology's lifecycle.

Anagbogu (2025) and Salami and Nwankwo (2024) suggest that Nigeria should draw inspiration from global best practices, such as the EU's risk-based approach, to ensure its AI systems meet international standards.

Furthermore, robust enforcement by the Nigeria Data Protection Commission (NDPC) is deemed essential, as laws alone do not suffice without active intervention, audits, and enforcement actions. Salami and Nwankwo (2024) also uniquely recommend that until the NDPR and NDPA are harmonized, they should be interpreted in a complementary fashion to avoid regulatory uncertainty.

Further, legislative action must be supported by practical measures, such as investing in infrastructure, developing a skilled workforce, and enhancing the technical capacity of regulatory bodies (Okeke et al., 2024).

To ensure equitable healthcare outcomes inspired by AI, it is important to prioritize fairness, transparency, and trust in algorithmic decision-making. Bias mitigation entails rigorous analysis and recalibration of AI models using diverse, representative datasets that capture the complexity of patient demographics (Keshta, 2022). Leveraging bias detection tools is crucial for guaranteeing unbiased treatment across disparate patient populations. Furthermore, transparent AI decision-making processes, facilitated by Explainable AI (XAI) methodologies, are essential for cultivating trust among healthcare stakeholders, thereby fostering a collaborative and reliable partnership (Olatunji et al., 2022; Rahman et al., 2022).

The creation of healthcare AI systems that are ethically sound, legally compliant, and technologically advanced requires a convergent effort from several fields of expertise. Continual research and innovation are important in addressing complex challenges, including enhancing data integrity, integrating domain-specific expertise, and developing effective incentive structures for data exchange (Mosaiyebzadeh et al., 2023). The facilitation of data sharing is especially vital for Federated Learning, where collaborative data exchange between organizations can significantly augment AI model performance and accuracy (Khalid et al., 2023).

As regulatory frameworks continue to adapt to the trends, they must integrate ethical principles such as fairness, patient self-determination, and bias reduction to mitigate

healthcare inequities (Williams & Prybutok, 2024). The intricacies of liability and accountability in AI-informed decision-making underscore the necessity for dynamic regulatory systems that strike a balance between safeguarding patient data and fostering innovation. To guarantee AI safety, efficacy, and alignment with societal norms, ongoing surveillance, transparency, and a risk-informed approach are essential (Reddy et al., 2019).

Stakeholders from diverse backgrounds, including technologists, healthcare professionals, ethicists, and patients, must be involved in AI development to ensure that solutions prioritize patient-centered care, dignity, and values, ultimately leading to better health outcomes (Williams & Prybutok, 2024).

V—CONCLUSION

The integration of artificial intelligence (AI) and healthcare has revolutionized medical practice, enabling precise diagnoses and enhanced patient outcomes. However, scholars universally acknowledge that realizing AI's full potential in healthcare necessitates addressing inherent challenges, including safeguarding patient data privacy and security, mitigating biases in algorithmic decision-making, and considering the ethical implications of AI adoption. By prioritizing these important issues, researchers and developers can foster collaborative innovation, ultimately yielding breakthroughs that utilize the transformative power of AI to create a future where healthcare is more tailored, precise, and universally accessible.

In furtherance, the S²AI framework offers a promising solution for ensuring the confidentiality and integrity of patient data in AI-driven healthcare applications. By adopting this framework, healthcare providers can confidently harness the benefits of AI to improve patient care while adhering to stringent data protection standards and ethical guidelines.

To fully realize the potential of AI in healthcare, it is crucial to implement a comprehensive strategy that integrates robust privacy safeguards, rigorous data protection protocols, and continuous ethical monitoring, thereby ensuring the protection of patient rights and interests.

REFERENCES

1. Abramoff, M. D., Tobey, D., & Char, D. S. (2020). Lessons learned about autonomous AI: Finding a safe, efficacious and ethical path through the development process. *American Journal of Ophthalmology*, 214, 134–142. <https://doi.org/10.1016/j.ajo.2020.02.016>
2. Achiam, J., Adler, S., Agarwal, S., Ahmad, L., Akkaya, I., et al. (2024). GPT-4 technical report. arXiv, arXiv:2303.08774.
3. Adedeji, K. A. (2025). Addressing data privacy concerns in artificial intelligence systems: Regulatory mechanisms in Nigeria. SSRN. <https://ssrn.com/abstract=5222866>
4. Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., et al. (2023). Revolutionizing healthcare: The role of artificial intelligence in clinical practice. *BMC Medical Education*, 23, 689. <https://doi.org/10.1186/s12909-023-04698-z>
5. American Medical Association. (n.d.). Informed consent. <https://www.ama-assn.org/delivering-care/ethics/informed-consent>
6. American Society of Human Genetics. (n.d.). The Genetic Information Nondiscrimination Act (GINA). <https://www.eeoc.gov/genetic-information-discrimination>
7. Anagbogu, P. (2025). *Artificial intelligence generated contents and data protection in Nigeria*. SSRN. <https://ssrn.com/abstract=5050781>
8. An, Q., Rahman, S., Zhou, J., & Kang, J. J. (2023). A comprehensive review on machine learning in healthcare industry: Classification, restrictions, opportunities and challenges. *Sensors*, 23(9), Article 4178. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10180678/>
9. Anthimopoulos, M., Christodoulidis, S., Ebner, L., Christe, A., & Mougiakakou, S. (2016). Lung pattern classification for interstitial lung

- diseases using a deep convolutional neural network. *IEEE Transactions on Medical Imaging*, 35, 1207–1216. <https://doi.org/10.1109/TMI.2016.2535865>
10. Arcadu, F., Benmansour, F., Maunz, A., Willis, J., Haskova, Z., & Prunotto, M. (2019). Deep learning algorithm predicts diabetic retinopathy progression in individual patients. *NPJ Digital Medicine*, 2, Article 92. <https://doi.org/10.1038/s41746-019-0172-3>
 11. Bakkar, N., Kovalik, T., Lorenzini, I., et al. (2018). Artificial intelligence in neurodegenerative disease research: Use of IBM Watson to identify additional RNA-binding proteins altered in amyotrophic lateral sclerosis. *Acta Neuropathologica*, 135, 227–247. <https://doi.org/10.1007/s00401-017-1785-8>
 12. Bayardo, R. J., & Agrawal, A. (2005). Data privacy through optimal k-anonymization. In *Proceedings 21st International Conference on Data Engineering, 2005 (ICDE 2005)*. IEEE.
 13. Bennett, S. M., Ehrenreich-May, J., Litz, B. T., Boisseau, C. L., & Barlow, D. H. (2012). Cognitive and behavioral practice. *Cognitive and Behavioral Practice*, 19(1), 161-173. <https://doi.org/10.1016/j.cbpra.2011.01.002>
 14. Bharati, S., Mondal, M. R. H., Podder, P., & Prasath, V. B. S. (2022). Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems*, 18(1-2), 19-35. <https://doi.org/10.3233/HIS-220006>
 15. Bohr, A., & Memarzadeh, K. (2020). The rise of artificial intelligence in healthcare applications. In *Artificial Intelligence in Healthcare* (pp. 25–60). Academic Press. <https://doi.org/10.1016/B978-0-12-818438-7.00002-2>
 16. Bonawitz, K., Kairouz, P., McMahan, B., & Ramage, D. (2021). Federated learning and privacy: Building privacy-preserving systems for machine learning and data science on decentralized data. *Queue*, 19(5), 87–114. <https://queue.acm.org/detail.cfm?id=3501293>

17. Brown, J. M., Campbell, J. P., Beers, A., et al. (2018). Automated diagnosis of plus disease in retinopathy of prematurity using deep convolutional neural networks. *JAMA Ophthalmology*, 136(7), 803–810.
18. Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care—Addressing ethical challenges. *New England Journal of Medicine*, 378(11), 981-983.
19. Chon, Z., & Alexander, D. (2023, August). Data governance frameworks for ensuring data integrity in clinical trials informatics [Conference presentation]. University of Hong Kong, China. Retrieved from https://www.researchgate.net/publication/373214562_Data_Governance_Frameworks_for_Ensuring_Data_Integrity_in_Clinical_Trials_Informatics
20. Dhoriya, A. (2024, August 25). Understanding transparency and control in consumer data use: A beginner's guide. <https://abhisekdhoriya.com/transparency-and-control-in-consumer-data-use/>
21. Duca, A. L., Bacciu, C., & Marchetti, A. (2016). How distributed ledgers can transform healthcare applications. *Blockchain Engineering*, 25.
22. Dyda, A., Purcell, M., et al. (2021). Differential privacy for public health data: An innovative tool to optimize information sharing while protecting data confidentiality. *Patterns*, 2(12), Article 100366. <https://doi.org/10.1016/j.patter.2021.100366>
23. Ekins, S., Mestres, J., & Testa, B. (2007). In silico pharmacology for drug discovery: Methods for virtual ligand screening and profiling. *British Journal of Pharmacology*, 152(1), 9–20. <https://doi.org/10.1038/sj.bjp.0707305>
24. Ferrer, F. (2023, March 7). Privacy preserving analytics. LinkedIn. <https://www.linkedin.com/pulse/privacy-preserving-analytics-fernando-ferrer>
25. Festor, P., Nagendran, M., Gordon, A. C., Faisal, A. A., & Komorowski, M. (2023). Evaluating the human safety net: Observational study of physician

- responses to unsafe AI recommendations in high-fidelity simulation. medRxiv. doi: 10.03.23296437
26. Gaid, M. L., & Salloum, S. A. (2021). Homomorphic encryption. In A. E. Hassanien, et al. (Eds.), *Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021)* (pp. 634-642). Springer. https://doi.org/10.1007/978-3-030-76346-6_56
 27. Garg, A., & Mago, V. (2021). Role of machine learning in medical research: A survey. *Computer Science Review*, 40, Article 100370. <https://doi.org/10.1016/j.cosrev.2021.100370>
 28. Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial Intelligence in Healthcare* (pp. 295-336).
 29. Hajrahimi, N., Hejazi Dehaghani, S. M., & Sheikhtaheri, A. (2013). Health information security: A case study of three selected medical centers in Iran. *Acta Informatica Medica*, 21(1), 42-45.
 30. Hall, J. L., & MacDraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs*, 33(2). <https://doi.org/10.1377/hlthaff.2013.0997>
 31. Hall, J. L., & McGraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs*, 33(2), 216–221.
 32. Hastings, M. C. (2021). *Secure multi-party computation in practice* [Doctoral dissertation, University of Pennsylvania]. Retrieved from <https://www.sciencedirect.com/science/article/pii/S001048252300313X#b72>
 33. Hirani, R., Noruzi, K., Khuram, H., Hussaini, A. S., Aifuwa, E. I., Ely, K. E., et al. (2024). Artificial intelligence and healthcare: A journey through history, present innovations, and future possibilities. *Life*, 14(5), 557. doi: 10.3390/life14050557

34. Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98. <https://doi.org/10.1080/13600834.2019.1573501>
35. Jangde, P., & Mishra, D. K. (2011). A secure multiparty computation solution to healthcare frauds and abuses. In *2011 Second International Conference on Intelligent Systems, Modelling and Simulation* (pp. 139–142). IEEE.
36. Jumper, J., Evans, R., Pritzel, A., et al. (2021). Highly accurate protein structure prediction with AlphaFold. *Nature*, 596, 583–589. <https://doi.org/10.1038/s41586-021-03819-2>
37. Keane, P. A., & Topol, E. J. (2018). With an eye to AI and autonomous diagnosis. *npj Digital Medicine*, 1(1), 40. doi: 10.1038/s41746-018-0048-y
38. Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. *Information Medicine Unlocked*, 30, 100903.
39. Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine*, 158, 106848. <https://doi.org/10.1016/j.combiomed.2023.106848>
40. Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine*, 158, 106848. <https://doi.org/10.1016/j.combiomed.2023.106848>
41. Kihara, Y., Heeren, T. F. C., Lee, C. S., et al. (2019). Estimating retinal sensitivity using optical coherence tomography with deep-learning algorithms in macular telangiectasia type 2. *JAMA Network Open*, 2(1), Article e188029. <https://doi.org/10.1001/jamanetworkopen.2018.8029>

42. Kirch, D. G., & Petelle, K. (2017). Addressing the physician shortage: The peril of ignoring demography. *JAMA*, 317(19), 1947–1948. <https://doi.org/10.1001/jama.2017.2714>
43. Kulikowski, C. A. (2019). Beginnings of artificial intelligence in medicine (AIM): Computational artifice assisting scientific inquiry and clinical art— With reflections on present AIM challenges. *Yearbook of Medical Informatics*, 28(1), 249–256. <https://doi.org/10.1055/s-0039-1677895>
44. Love-Koh, J. (2018). The future of precision medicine: Potential impacts for health technology assessment. *Pharmacoeconomics*, 36(12), 1439–1451. <https://doi.org/10.1007/s40273-018-0686-6>
45. Makhni, S., Cook, S. C., Williams, J. S., Umscheid, C. A., & Chin, M. H. (2022). Framework for integrating equity into machine learning models: A case study. *Chest*, 161(6), 1621-1627.
46. Markose, A., Krishnan, R., & Ramesh, M. (2016). Medical ethics. *Journal of Pharmacy & Bioallied Sciences*, 8(Suppl 1), S1–S4. <https://pubmed.ncbi.nlm.nih.gov/27829735/>
47. Marr, B. (2018, July 27). How is AI used in healthcare—5 powerful real-world examples that show the latest advances. *Forbes*. <https://www.forbes.com/sites/bernardmarr/2018/07/27/how-is-ai-used-in-healthcare-5-powerful-real-world-examples-that-show-the-latest-advances/>
48. Martineau, K. (2022, August 24). What is federated learning?. IBM Research. <https://research.ibm.com/blog/what-is-federated-learning>
49. Maxeiner, J. R. (1995). Freedom of information and the EU data protection directive. *Fed. Comm. LJ*, 48, 93.
50. May, T. (2023, October 26). An overview of approaches to privacy-preserving data sharing. *Medium Blog*. <https://medium.com/datavant/an-overview-of-approaches-to-privacy-preserving-data-sharing-64fc5d4a9b48>

51. Mehta, J., & Majumdar, A. (2017). Rodeo: Robust de-aliasing autoencoder for real-time medical image reconstruction. *Pattern Recognition*, 63, 499–510.
<https://www.sciencedirect.com/science/article/abs/pii/S0031320316302850>
52. Meskó, B., & Topol, E. J. (2023). The imperative for regulatory oversight of large language models (or generative AI) in healthcare. *npj Digital Medicine*, 6, 120.
53. Miller, R. A., Pople, H. E., Jr., & Myers, J. D. (1982). Internist-I, an experimental computer-based diagnostic consultant for general internal medicine. *New England Journal of Medicine*, 307(8), 468-476.
<https://doi.org/10.1056/NEJM198208193070803>
54. Mintz, Y., & Brodie, R. (2019). Introduction to artificial intelligence in medicine. *Minimally Invasive Therapy & Allied Technologies*, 28(2), 73–81.
<https://doi.org/10.1080/13645706.2019.1575882>
55. Morley, J., Machado, C. C. V., Burr, C., Cowls, J., Taddeo, M., & Floridi, L. (2019). The debate on the ethics of AI in health care: A reconstruction and critical review. *Social Science Research Network*.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486518
56. Morris, D. (2023, January 3). How encryption works to preserve data privacy. *Dataversity*. <https://www.dataversity.net/how-encryption-works-to-preserve-data-privacy/>
57. Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Sheng, Q. Z., Han, M., Zhao, L., Sannino, G., Ranieri, C. M., Ueyama, J., & Batista, D. M. (2023). Privacy-enhancing technologies in federated learning for the Internet of Healthcare Things: A survey. *Electronics*, 12, 2703.
58. Murdoch, B. (2021). Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics*, 22(1), 122.

59. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. U.S. Government Printing Office.
60. Near, J., Darais, D., & Boeckl, K. (2020, July 27). Differential privacy: Privacy-preserving data analysis. Introduction to our blog series. National Institute of Standards and Technology. <https://www.nist.gov/blogs/cybersecurity-insights/differential-privacy-privacy-preserving-data-analysis-introduction-our>
61. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447-453.
62. Okeke, O. E., Agbonghae, B. E., & Green, A. U. (2024). Artificial Intelligence and Security of the People in Nigeria. *Journal of Public and Human Rights Law*, 1(2), 158–167.
63. Olatunji, I. E., Rauch, J., Katzensteiner, M., & Khosla, M. (2022). A review of anonymization for healthcare data. *Big Data*.
64. Pasquale, F. (2020, November 9). When medical robots fail: Malpractice principles for an era of automation. The Brookings Institution. <https://policycommons.net/artifacts/4143655/when-medical-robots-fail/4952762/>
65. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4(1), tyy001.
66. Radanliev, P., Santos, O., Brandon-Jones, A., & Joinson, A. (2024). Ethics and responsible AI deployment. *Frontiers in Artificial Intelligence*, 7, Article 1377011. <https://doi.org/10.3389/frai.2024.1377011>

67. Rahman, A., Hossain, M. S., Muhammad, G., Kundu, D., Debnath, T., Rahman, M. S., ... & Band, S. S. (2022). Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges and open issues. *Cluster Computing*, 26, 2271–2311.
68. Ram Mohan Rao, P., Murali Krishna, S., & Siva Kumar, A.P. (2018). Privacy preservation techniques in big data analytics: A survey. *J Big Data*, 5, 33. <https://doi.org/10.1186/s40537-018-0141-8>
69. Rashid, D., Hirani, R., Khessib, S., Ali, N., & Etienne, M. (2024). Unveiling biases of artificial intelligence in healthcare: Navigating the promise and pitfalls. *Injury*, 55, 111358.
70. Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2019). A governance model for the application of AI in health care. *Journal of the American Medical Informatics Association*, 27, 491–497.
71. Richardson, J. W., Smith, C., Curtis, S., Watson, S. E., Zhu, X., Barry, B. A., & Sharp, R. R. (2021). Patient apprehensions about the use of artificial intelligence in healthcare. *Npj Digital Medicine*, 4, 140. <https://doi.org/10.1038/s41746-021-00508-2>
72. Rojas, J. C., Fahrenbach, J., Makhni, S., Cook, S. C., Williams, J. S., Umscheid, C. A., & Chin, M. H. (2022). Framework for integrating equity into machine learning models: A case study. *Chest*, 161(6), 1621-1627.
73. Roy, S. (2022). Privacy prevention of healthcare data using AI. *Journal of Data Acquisition and Processing*, 37(3), 2022. <https://doi.org/10.5281/zenodo.7699408>
74. Salami, E., & Nwankwo, I. (2024). Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer. *African Journal on Privacy & Data Protection*, 1(1), 220–247. <https://doi.org/10.29053/ajpdp.v1i1.0011>
75. Scheibner, J., Ienca, M., & Vayena, E. (2022). Health data privacy through homomorphic encryption and distributed ledger computing: An ethical-legal

- qualitative expert assessment study. *BMC Medical Ethics*, 23(1), 121. <https://doi.org/10.1186/s12910-022-00852-2>
76. Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J. R., Raisaro, J. L., Hubaux, J.-P., Fellay, J., & Vayena, E. (2020). Data protection and ethics requirements for multisite research with health data: A comparative examination of legislative governance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences*, 7(1), lsa010. <https://doi.org/10.1093/jlb/lsa010>
77. Schlemper, J., Caballero, J., Hajnal, J. V., Price, A., & Rueckert, D. (2017). A deep cascade of convolutional neural networks for MR image reconstruction. In *Information Processing in Medical Imaging: 25th International Conference, IPMI 2017* (pp. 647–658). Springer. https://doi.org/10.1007/978-3-319-59050-9_51
78. Sheller, M. J., Edwards, B., Reina, G. A., et al. (2020). Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. *Scientific Reports*, 10(1), 1–12.
79. Sheng, Q. Z., Han, M., Zhao, L., et al. (2023). Privacy-enhancing technologies in federated learning for the Internet of Healthcare Things: A survey. *Electronics*, 12(12), 2703. <https://doi.org/10.3390/electronics12122703>
80. Shortliffe, E. H. (1977, October 3–5). *Mycin: A knowledge-based computer program applied to infectious diseases*. Proceedings of the Annual Symposium on Computer Application in Medical Care, Washington, DC, USA, pp. 66–69.
81. Singhal, S. (2024). Data privacy, compliance, and security including AI ML: Healthcare. In *Practical Applications of Data Processing, Algorithms, and Modeling* (pp. 111–126). IGI Global. <https://doi.org/10.4018/979-8-3693-2909-2.ch009>

82. The Laboratory of Computer Science | DXplain. (n.d.). Using decision support to help explain clinical manifestations of disease. <https://www.mghlcs.org/projects/dxplain>
83. Tholoniati, P. (2023, December 22). Have your data and hide it too: An introduction to differential privacy. Cloudflare. <https://blog.cloudflare.com/have-your-data-and-hide-it-too-an-introduction-to-differential-privacy/>
84. Tilala, M. H., Chenchala, P. K., Choppadandi, A., et al. (2024). Ethical considerations in the use of artificial intelligence and machine learning in health care: A comprehensive review. *Cureus*, 16(6), e62443. doi: 10.7759/cureus.62443
85. Tom, E., Keane, P. A., Blazes, M., et al. (2020). Protecting data privacy in the age of AI-enabled ophthalmology. *Translational Vision Science & Technology*, 9(2), 36. <https://doi.org/10.1167/tvst.9.2.36>
86. Vation Ventures. (n.d.). Artificial intelligence: Definition, explanation, and use cases. Retrieved from <https://www.vationventures.com/glossary/artificial-intelligence-definition-explanation-and-use-cases#>
87. Walton, M. (2024). Implementing privacy-first approaches in AI data merchandising privacy-first approaches in AI data handling. Retrieved from https://www.researchgate.net/publication/386083241_Implementing_Privacy_First_Approaches_in_AI_Data_Merchandising_Privacy_First_Approaches_in_AI_Data_Handling
88. Warnat-Herresthal, S., Schultze, H., Shastry, K. L., et al. (2021). Swarm learning for decentralized and confidential clinical machine learning. *Nature*, 594(7862), 265–270.
89. Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*, 14(2), 675. <https://doi.org/10.3390/app14020675>

90. Yan, Z., Zhan, Y., Peng, Z., et al. (2016). Multi-instance deep learning: Discover discriminative local anatomies for body-part recognition. *IEEE Transactions on Medical Imaging*, 35, 1332–1343. <https://doi.org/10.1109/TMI.2016.2524985>