


Review

Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare

Steven M. Williamson¹ and Victor Prybutok^{2,*} ¹ Department of Information Science, College of Information, University of North Texas, Denton, TX 76203, USA; stevenwilliamson@my.unt.edu² Department of Information Technology and Decision Sciences, G. Brint Ryan College of Business, University of North Texas, Denton, TX 76203, USA

* Correspondence: prybutok@unt.edu

Abstract: Integrating Artificial Intelligence (AI) in healthcare represents a transformative shift with substantial potential for enhancing patient care. This paper critically examines this integration, confronting significant ethical, legal, and technological challenges, particularly in patient privacy, decision-making autonomy, and data integrity. A structured exploration of these issues focuses on Differential Privacy as a critical method for preserving patient confidentiality in AI-driven healthcare systems. We analyze the balance between privacy preservation and the practical utility of healthcare data, emphasizing the effectiveness of encryption, Differential Privacy, and mixed-model approaches. The paper navigates the complex ethical and legal frameworks essential for AI integration in healthcare. We comprehensively examine patient rights and the nuances of informed consent, along with the challenges of harmonizing advanced technologies like blockchain with the General Data Protection Regulation (GDPR). The issue of algorithmic bias in healthcare is also explored, underscoring the urgent need for effective bias detection and mitigation strategies to build patient trust. The evolving roles of decentralized data sharing, regulatory frameworks, and patient agency are discussed in depth. Advocating for an interdisciplinary, multi-stakeholder approach and responsive governance, the paper aims to align healthcare AI with ethical principles, prioritize patient-centered outcomes, and steer AI towards responsible and equitable enhancements in patient care.

Keywords: Artificial Intelligence (AI) in healthcare; Differential Privacy (DP); data privacy and security; algorithmic bias and discrimination; patient agency; regulatory oversight; blockchain technology; Federated Learning; ethical AI implementation; patient-centric outcomes



Citation: Williamson, S.M.; Prybutok, V. Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Appl. Sci.* **2024**, *14*, 675. <https://doi.org/10.3390/app14020675>

Academic Editors: Chilukuri K. Mohan and Paris Kitsos

Received: 30 October 2023

Revised: 9 December 2023

Accepted: 11 January 2024

Published: 12 January 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Integrating Artificial Intelligence (AI) in healthcare marks a significant milestone, signaling the advent of a new era in precision medicine. This transformative shift holds immense promise for revolutionizing patient care, offering advancements that were once considered futuristic. By harnessing AI's capabilities, healthcare systems stand on the brink of a paradigm shift characterized by enhanced diagnostic accuracy, personalized treatment strategies, and increased efficiency in healthcare delivery. The ability of AI to process and analyze vast health data sets with unparalleled precision heralds a new age of medicine where disease prediction models are significantly more accurate, therapies are increasingly targeted to individual patient needs, and patient outcomes are markedly improved. This integration of AI into healthcare goes beyond mere technological advancement; it represents a fundamental change in the approach to patient care, where data-driven insights and machine learning algorithms have the potential to uncover patterns and solutions previously hidden in vast amounts of health data. From predicting patient risks to tailoring treatment plans, AI's impact is profound, enabling healthcare providers to make more

informed decisions and offer care that is both effective and personalized. However, the integration of AI into healthcare has its challenges. Foremost among these is the need to safeguard patient privacy in an environment where data are both a valuable resource and a potential vulnerability. Handling sensitive health information by AI systems raises significant concerns about privacy, data protection, and the risk of data breaches. Additionally, the increasing reliance on AI for decision-making in healthcare poses questions about maintaining human autonomy in medical decisions. Ensuring that AI assists rather than overrides the judgment of healthcare professionals is crucial for maintaining the human element in healthcare.

This literature review investigates the specific privacy challenges associated with the deployment of AI in healthcare, with a focus on large-scale data processing, Differential Privacy, and anonymization techniques. It also explores how these challenges contribute to a gap between patients' perceptions and privacy and security scenarios in AI-integrated healthcare systems. The sensitive nature of health data and their potential for misuse necessitate urgent attention to these issues. AI's reliance on extensive patient data amplifies concerns about data security, informed consent, data ownership, and the risk of unauthorized exploitation. In addition to privacy concerns, this review expands its scope to consider broader ethical issues, such as the impact of AI on healthcare decision-making autonomy and the potential for algorithmic bias and discrimination. These concerns are particularly crucial as AI systems become more integral to healthcare, raising questions about the transparency and fairness of decision-making processes, especially for diverse patient populations.

Addressing these complex issues, our review underscores the importance of transparent communication with patients and the public to demystify AI's role in healthcare. This approach aims to bridge the gap between perceived and actual AI applications in healthcare, addressing misconceptions and fostering informed understanding among patients and healthcare providers. Crucially, we draw upon key insights from works such as those by [1,2], which delve into the privacy risks of private entities' AI control and the ethical challenges in its implementation. Through this comprehensive exploration, our review aims to develop balanced strategies and policies that optimize the benefits of AI while protecting patient rights and trust. Central to our discussion is advocating for a nuanced understanding of AI's role in healthcare, particularly in privacy, data security, and ethical integration, to guide effective policy-making and strategic development in this essential field.

2. Methodology

2.1. Protocol

In conducting this literature review, we adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines outlined in [3]. These guidelines provided a robust framework for conducting a systematic approach to the literature search, ensuring a comprehensive and unbiased review of the existing literature on integrating Artificial Intelligence (AI) in healthcare. To enhance the efficiency and effectiveness of our literature search, we incorporated advanced AI research tools. These tools were guided by specific Boolean search queries composed of carefully selected keywords and common abbreviations, ensuring a focused and relevant literature search. The primary keywords used in our search strategy included terms such as 'Artificial Intelligence', 'AI', 'Systemic', 'Oversight', 'Healthcare', 'Decision-Making', 'Autonomy', 'Dignity', 'Advancing', 'Data', 'Anonymization', 'Protection', 'Promoting', 'Transparency', 'Dialogue', 'Privacy', 'Disparities', and 'Patient Understanding'. This comprehensive approach allowed us to capture studies pertinent to our research objectives. Table 1 illustrates the detailed process of our systematic review, outlining the steps involved, the number of articles reviewed at each stage, the AI tools utilized, and the specific keywords and abbreviations that guided our search. This table provides a clear overview of our methodical approach and the extensive scope of our literature review.

Table 1. Systematic review process for AI in healthcare research.

Step in Review Process	Description	Number of Articles	Actions Taken	AI Tools Used	Keywords Used	Abbreviations Used
Identification	Initial search of information sources using AI tools, yielding a total of 875 articles	875	Used AI tools for initial search	Elicit, SciSpace, Mirrorthink	'Artificial Intelligence', 'Healthcare', 'Data Privacy and Security', 'Differential Privacy', 'Algorithmic Bias', 'Patient Agency', 'Regulatory Oversight', 'Ethical AI', 'Data Anonymization', 'Transparency', 'Patient Perspectives'	'AI', 'DP', 'Bias'
Screening	Screening of 875 articles, removing 483 duplicates, manually reviewing 392 for relevance	392	Removed duplicates; reviewed abstracts and titles	Elicit, SciSpace, Mirrorthink	'Privacy Challenges', 'Data Security', 'Algorithmic Discrimination', 'Healthcare Decision-Making', 'AI Ethics', 'Data Ownership', 'Informed Consent', 'Fairness in AI', 'Patient Understanding', 'Healthcare Autonomy'	'AI', 'DP', 'Bias'
Eligibility	Assessment of 392 articles for eligibility based on specific criteria	392	Assessed articles for relevance to research question	Elicit, SciSpace, Mirrorthink	'Differential Privacy', 'Patient Agency', 'Algorithmic Bias', 'Data Integrity', 'Regulatory Oversight', 'Ethical AI Implementation', 'Data Protection', 'AI Transparency', 'Healthcare Innovation', 'Patient-Centric Care'	'AI', 'DP', 'Bias'
Included	Final selection of 27 articles suitable for review, after full-text review and applying inclusion criteria	27	Reviewed full-text; applied inclusion criteria	Elicit, SciSpace, Mirrorthink	'AI in Healthcare', 'Ethical Challenges in AI', 'Privacy and Security in Healthcare AI', 'Patient-Centric AI Solutions', 'Regulatory Frameworks for AI', 'AI Bias Mitigation', 'AI and Patient Rights', 'Data Anonymization Techniques', 'AI Decision-Making', 'Transparency in AI'	'AI', 'DP', 'Bias'

The rationale for our keyword selection was strategically crafted to align with the core objectives of our research, which delves into the integration of AI in healthcare and its associated challenges. Keywords such as 'Artificial Intelligence' and 'Healthcare' directly target the central theme, addressing the intersection of AI and healthcare. To explore privacy concerns, keywords like 'Differential Privacy' and 'Data Security' were chosen, emphasizing how AI systems manage and protect sensitive patient information. 'Algorithmic Bias' and 'Ethical AI Implementation' were selected to shed light on potential biases in AI algorithms and the need for ethical frameworks. 'Patient Agency' and 'Patient-Centric Care' were included to ensure our review encapsulates AI's impact on patient autonomy and decision-making. Lastly, 'Regulatory Oversight' and 'AI Transparency' were incorporated to investigate AI's legal and clarity aspects in healthcare, focusing on transparent operations and robust regulatory frameworks.

Our literature review's inclusion and exclusion criteria were stringently defined to ensure a focused and relevant collection of studies. We included peer-reviewed articles published from 2018 to 2023, reflecting contemporary developments in this rapidly evolving field. The focus was on articles that addressed AI integration in healthcare, particularly

those delving into its ethical, legal, and practical implications. Studies highlighting patient privacy, data security, algorithmic bias, and regulatory challenges were prioritized. Conversely, we excluded articles published outside the specified date range, non-peer-reviewed articles, opinion pieces, and editorials to uphold academic rigor. Studies not directly addressing AI in healthcare or lacking a focus on the specified dimensions were also excluded. Due to language constraints, non-English articles were not considered.

The PRISMA checklist served as a strategic tool in structuring the review process. It guided the identification, screening, eligibility assessment, and inclusion of studies, ensuring that each step was conducted systematically and transparently. We meticulously examined the titles and abstracts of articles using the keywords above and their variants, including full terms and abbreviations, such as 'AI' for 'Artificial Intelligence'. This dual approach ensured that we did not overlook relevant studies due to variations in terminology. Simultaneously, the AI research tools were utilized to automate and streamline the search and selection processes. These tools allowed us to efficiently scan a large volume of literature and identify articles matching our specific search terms and exclusion criteria. By combining the methodical rigor of the PRISMA guidelines with the advanced capabilities of AI research tools, we conducted a thorough and systematic literature review that contributed valuable insights into the role of AI in healthcare.

2.2. Information Sources

The literature search for this study was conducted using a comprehensive and systematic approach, using various electronic databases and advanced Artificial Intelligence (AI) research tools. These tools enhanced the search process's efficiency and effectiveness, allowing for a more nuanced and targeted exploration of academic literature. One of the primary AI tools used was Elicit, which performs semantic searches across the vast corpus of academic papers available in the Semantic Scholar Academic Graph dataset. Elicit employs a unique model that stores embeddings of titles and abstracts in a vector database. When a research query—comprising our specific keywords such as 'Artificial Intelligence', 'AI', 'Healthcare', and others—is entered, it is embedded using the same model, and the vector database returns the closest embeddings, thus identifying the most relevant papers. Another AI assistant used in our search was SciSpace, which leverages the RETA-LLM model for retrieval-augmented large language model systems. This model enhances the search process by incorporating information retrieval systems that generate factual responses through content retrieved from external corpora. It is particularly adept at answering in-domain questions that require more than just the world knowledge stored in parameters. Additionally, we employed Mirrorthink, a platform that utilizes GPT-4, a state-of-the-art neural network capable of generating natural language responses to queries. Mirrorthink's integration with databases such as PubMed ensures the accuracy and reliability of the data and results obtained.

These AI research tools were used to search various electronic databases, employing a strategic combination of full terms and abbreviations of our selected keywords. This allowed for a more comprehensive and efficient exploration of the available literature, ensuring that the most relevant and up-to-date studies were included in the review. Using these advanced AI tools in the literature search process represents a novel approach to conducting literature reviews. It demonstrates the potential of AI to significantly contribute to academic research by streamlining the identification and retrieval of pertinent studies, thereby facilitating a more thorough and systematic review of the literature on AI in healthcare.

2.3. Eligibility Criteria

This review encompasses peer-reviewed articles published within the timeframe of 2018–2023. These articles were selected by specific inclusion criteria, emphasizing the semantic similarity of the article's title and abstract to the research question. Re-ranking the papers based on relevance ensured that the most pertinent studies were included in the

review. The results were analyzed through a systematic, three-step process. The first step utilized AI research tools to gather a significant number of articles. During this phase, the titles and abstracts of the articles were meticulously examined for specific search terms and exclusion criteria. To guarantee the uniqueness of the articles, duplicates were automatically removed by the AI tools and then manually by the researchers. In the second step, the articles were independently screened based on their title and abstract to identify those that generally met the inclusion criteria. This step involved a comprehensive assessment of each article by reading the complete text, ensuring that only the most pertinent studies were chosen for further analysis. The final step involved retrieving the full-text articles and conducting data extraction. This process was streamlined by a modified template from the PRISMA method, which offered a structured approach to data extraction. This phase also employed AI tools to extract insights and information from the chosen articles. This innovative approach to data extraction enhanced the process's efficiency and ensured the extracted data's accuracy and reliability. This methodical approach to data analysis, supported by AI tools and guided by the PRISMA method, ensured a thorough and accurate analysis of the articles. The use of in-text and narrative citations further strengthened the credibility of the analysis.

2.4. Results

The initial search of information sources yielded 875 articles from various databases, all of which were deemed relevant to the research question by the AI tool. In the second step, 483 duplicate articles were removed, and the abstracts of the remaining 392 articles were manually reviewed for relevance to the research question. However, 300 of these articles were found to be outside the scope of the review. In the third step, the remaining 92 articles were thoroughly reviewed. Out of these, 65 were excluded for various reasons: some were not related to healthcare, some did not discuss AI, some did not address privacy challenges, some did not discuss large-scale data processing, Differential Privacy, or anonymization schemes, some did not discuss patient perceptions, some were published before the specified date range, some were not published in English, and some had low quality or a high risk of bias. After this rigorous screening process, only 27 of the original 875 articles were deemed suitable for review using the PRISMA template, as shown in Figure 1. This methodical approach ensured that only the most relevant and high-quality articles were included in the review, enhancing the strength and validity of the research findings.

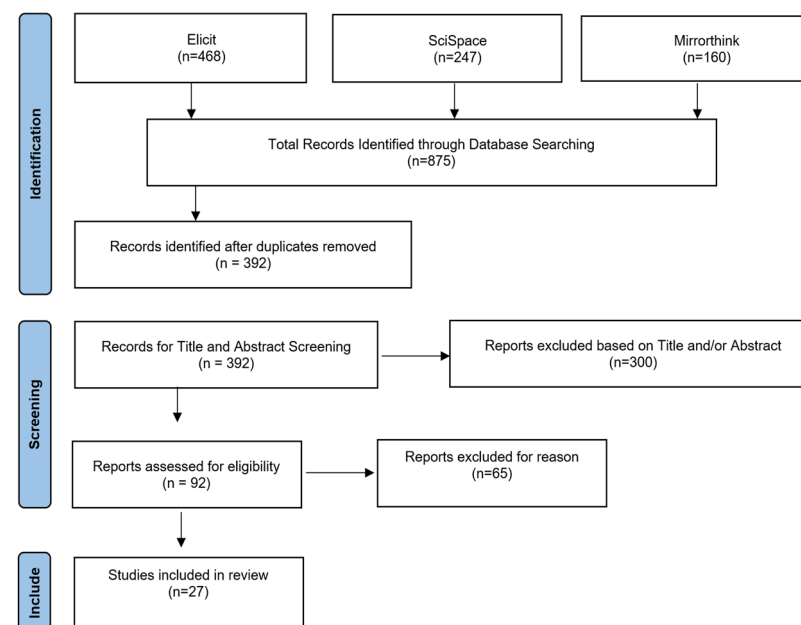


Figure 1. Process map of research methodology.

3. Transformative Impact and Ethical Implications of AI in Healthcare

3.1. AI's Capabilities and Its Impact on Healthcare

Integrating Artificial Intelligence (AI) into healthcare, particularly in data processing and analysis, is heralding a new era of medical care. This integration is not just about technological advancement but also encompasses a profound shift in the paradigm of patient care, providing opportunities to enhance healthcare delivery through more effective and efficient practices. However, this transformation is accompanied by intricate ethical challenges that must be navigated with caution and foresight. AI's capabilities in healthcare are extensive and diverse, ranging from diagnostics to treatment strategies and healthcare administration. For instance, AI systems have shown remarkable proficiency in structuring vast medical data, identifying clinical patterns, and validating medical hypotheses. This capability has led to improvements in healthcare quality and efficiency, alleviating the workload of healthcare professionals. The application of AI to making complex clinical decisions, particularly those that hinge on patient preferences, is a significant development. In scenarios like cardio-pulmonary resuscitation and determining Do Not Attempt to Resuscitate (DNAR) status, AI can offer computational assistance that aligns with patient preferences while mitigating human biases in decision-making under stress and time pressure [4–6].

The advancement of AI in healthcare has also been instrumental in enhancing diagnostic accuracy, tailoring personalized treatment strategies, and improving patient outcomes. AI's predictive capabilities in healthcare are particularly noteworthy, enabling proactive interventions and contributing to public health by identifying potential health risks and disease patterns. These capabilities are facilitated by AI's ability to process and analyze extensive datasets, including patient histories, diagnostic information, and treatment outcomes. As AI models become increasingly sophisticated and integrated into clinical settings, they necessitate a strong emphasis on data integrity and security. However, the reliance on extensive health data for AI algorithms brings critical ethical challenges to the fore. These include concerns related to patient privacy, decision-making autonomy, and data integrity. The need for large volumes of data to effectively train and operate AI systems poses inherent risks of privacy infringement. Therefore, there is a pressing need for careful management of health data collection, storage, and processing to uphold patient confidentiality. Moreover, using AI in disease prediction and risk factor analysis requires an ethical approach to handling sensitive health information. The potential for bias in AI algorithms, resulting from training on datasets not representative of the diverse patient population, could lead to inaccurate results and raise ethical concerns about equitable patient care [4–6].

The introduction of AI into healthcare decision-making processes also raises questions about the autonomy of healthcare providers and patients. The extent to which AI should influence medical decisions is a matter of ongoing debate, underscoring the need to balance AI recommendations with human judgment. While AI's capabilities in healthcare offer significant opportunities for enhancing patient care, addressing these ethical concerns is paramount. Responsible use of AI in healthcare requires navigating complex issues around privacy, bias, autonomy, and the integrity of decision-making processes. As AI continues to evolve, it is crucial to focus on ethical considerations to realize its full potential in a manner that aligns with the core values of healthcare [4].

Comprehensive insights into the complexities and ethical considerations surrounding the use of AI in healthcare are provided, especially in the context of decision-making processes for cardiopulmonary resuscitation and Do Not Attempt to Resuscitate (DNAR) status. The study conducted at a university hospital highlights the potential of AI to improve healthcare delivery and decision-making, especially in high-pressure, ethically sensitive situations. The AI systems discussed in the paper are primarily designed to assist with complex clinical decisions, especially those that depend heavily on patient preferences, such as resuscitation decisions. These systems can analyze vast data sets to generate suggestions consistent with patient preferences and likely outcomes, potentially reducing the impact of stress, time pressure, personal biases, and conflicts of interest that

may affect human decision-making. The paper acknowledges the challenges in healthcare decision-making, such as insufficient knowledge about patient preferences, time pressure, and personal biases that guide care considerations. It suggests that AI-based decision support could significantly improve the status quo by helping healthcare professionals and legal representatives make more informed decisions about a patient's DNAR status. The AI system would support rather than replace human decision-making, acting as a consultative tool to enhance decision-making [6].

However, the development of such AI systems is ethically demanding. It requires careful consideration of several preconditions, including the role of AI relative to human decision-making, legal liabilities, and the balance between algorithmic suggestions and human judgment [6]. The paper emphasizes the importance of transparency, explicability, bias monitoring, and user trust in ensuring the ethical application of AI in healthcare [4]. It also highlights the need for compatibility with hospital information systems, practical user training, and awareness of the limitations and risks of AI support in decision-making. The study's conclusion underscores the need for a well-defined ethical framework and evaluation standards for AI-based decision-support systems. As AI systems gain recognition for their accuracy and reliability, they raise critical questions at the intersection of medicine, ethics, and computer science, including bias, fairness, autonomy, and accountability [5]. The paper advocates for including various perspectives, particularly those of patients and legal representatives, in addressing these ethical and policy concerns to ensure the responsible use of AI in healthcare.

3.2. Addressing Privacy and Patient Agency through AI

The integration of AI in healthcare brings forth complex privacy challenges, particularly in the realms of data control and usage by private corporations. As AI systems increasingly handle sensitive patient data, concerns regarding the stewardship of this information by private entities become paramount. Establishing transparent and accountable data governance frameworks that respect patient privacy and agency is essential to addressing the potential for misuse or unauthorized exploitation of health data. These challenges underscore the need for a delicate balance between technological advancement and the protection of patient rights [1].

In the age of digital healthcare transformation, AI-driven systems are increasingly at the forefront of medical innovation. However, with this advancement come significant challenges concerning patient privacy and agency. The risk of privacy infringement due to the misuse of pseudo-anonymized patient data [7,8] is a primary concern. Sophisticated techniques can potentially re-engineer anonymized data to identify individuals, thus breaching patient confidentiality. The complexity of AI algorithms often makes it challenging to track patient data utilization within these systems [9,10], leading to potential misuse or a lack of transparency.

3.3. Implementing Ethical AI in Healthcare

Integrating Artificial Intelligence (AI) in healthcare represents a transformative shift in how medical services are delivered and managed. AI can improve diagnostic accuracy, personalize treatment plans, optimize resource allocation, and predict patient outcomes more precisely. However, the deployment of AI in healthcare must be cautiously approached due to the sensitive nature of medical data and the ethical implications surrounding its use [11]. Safeguarding patient data privacy is a critical issue in the healthcare sector, particularly with the integration of AI technologies that rely on medical records replete with sensitive personal information. Mishandling such data could result in significant privacy violations and misuse [7,12]. To mitigate these risks, a suite of sophisticated technologies has been developed to maintain the confidentiality and integrity of patient information while harnessing AI's capabilities.

Blockchain technology provides a secure, decentralized method for storing and managing healthcare data, utilizing a distributed ledger system to ensure that patient records

are immutable and verifiable, thereby thwarting unauthorized access and potential data breaches. It also enables secure data sharing among verified entities. In parallel, Federated Learning (FL) allows for training AI models on decentralized devices or servers that hold local data samples, negating the need to transfer sensitive patient data and thus reducing centralization concerns [13]. Homomorphic Encryption (HE) offers a solution for performing computations on encrypted data without decryption, allowing AI to process and learn from the data. At the same time, it remains encrypted, thus upholding privacy even when third-party analysis is required [9]. Lastly, Differential Privacy (DP) introduces controlled noise to data sets to obscure individual identities, permitting the training of AI models on population-representative data without compromising individual privacy [10]. Collectively, these technologies form a robust framework for protecting patient privacy in the age of AI-driven healthcare. Implementing these technologies reflects a commitment to ethical standards in healthcare AI. They address technical challenges and demonstrate a dedication to respecting and protecting patient rights, particularly regarding privacy and autonomy. As AI continues to evolve and become more integral to healthcare delivery, the role of these technologies in maintaining a balance between innovation and ethical responsibility becomes increasingly vital. They represent solutions to current challenges and a vision for a future where healthcare AI advances with ethical considerations, ensuring that patient welfare remains at the core of technological progress in the healthcare sector.

3.3.1. Blockchain Technology: Reinforcing Security and Transparency in Healthcare AI

Integrating Artificial Intelligence (AI) in healthcare marks a significant advancement in medical technology, offering potential benefits in enhancing patient care. However, it also introduces substantial ethical challenges concerning privacy and patient autonomy. These concerns necessitate the adoption of advanced technologies that can safeguard patient data while leveraging the benefits of AI in healthcare [11]. Blockchain technology has emerged as a promising solution to enhance data security and integrity in healthcare AI. Its decentralized nature eliminates the need for central authority, reducing the risk of a single point of failure that could compromise the entire system. In healthcare, blockchain can create a secure and unforgeable record of patient data transactions, ensuring that medical records are accurate, consistent, and tamper-proof. For a detailed exploration of how blockchain technology influences privacy and decision-making in AI healthcare, see the insights in Table 2. The blockchain application extends beyond just data storage; it can also facilitate secure data sharing between different healthcare stakeholders. Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, can automate the consent process for data sharing, ensuring that patient data are only accessed by authorized parties and under specific conditions agreed upon by the patient. Moreover, blockchain can be integrated with other technologies, such as AI and IoT devices, to enable secure and real-time monitoring of patient health data, providing healthcare professionals with reliable data for decision-making while preserving patient privacy [7,12].

Recent research underscores the collective potential of blockchain technology in bolstering the security and privacy of healthcare AI systems. The authors of [14] introduced an IoT-based model for secure big data transfer in healthcare, leveraging blockchain for data integrity and security. The authors of [15] proposed an architecture combining AI and blockchain to protect smart healthcare systems from data integrity attacks, focusing on wearable devices. The authors of [16] envisioned a healthcare metaverse where AI and blockchain work together to offer secure and efficient remote health monitoring and virtual consultations. The authors of [17] provided a bibliometric analysis highlighting the synergy between AI and blockchain in enhancing security and calling for more research to develop stable systems.

Table 2. Deeper impact of blockchain technology on privacy and decision-making in AI healthcare.

Feature	Impact on Privacy	Impact on Decision-Making	Additional Notes	Regulatory Considerations	User Experience Impact
Immutability	Enhances data confidentiality	Increases confidence in medical decisions	Limits data correction capabilities	Challenges in GDPR alignment	Improves patient trust in data security
Decentralization	Increases data privacy	Encourages collaborative decision-making	Reduces single points of failure	Diverse data control implications	Enhances data accessibility
Transparency	Boosts accountability and compliance	Supports informed decision-making	Increases administrative load	Facilitates audit trails	May overwhelm users with data details
Security	Prevents unauthorized data access	Relies on secure data for reliable decisions	Requires robust network security	Enhances data protection	Improves confidence in data use
Interoperability	Facilitates secure data exchange	Integrates diverse data for holistic decisions	Complex implementation across systems	Ensures seamless data flow	Enhances user experience with diverse data
Data Identifiability	Aligns with GDPR personal data criteria	Influences the scope of data use in decisions	Draws a line between personal and non-personal data; Challenges in identifying personal data	Central to GDPR compliance	Affects the perception of data privacy
Technical Evolution	Adapts to evolving privacy standards	Incorporates advanced decision-support tools	Includes zero-knowledge proofs, homomorphic encryption, and other privacy-preserving techniques	Must adapt to evolving GDPR standards	Enhances with technological advancements

These studies collectively advocate for integrating blockchain with AI to address security concerns, each contributing unique perspectives on system architecture, data transmission, and the application of smart contracts. By synthesizing their findings, it becomes evident that the convergence of these technologies can lead to innovative solutions for managing healthcare data with improved security and patient privacy. However, they also agree on the necessity for continued research to overcome data privacy, security, and trust challenges, ensuring the practical implementation of these advanced systems in real-world healthcare settings. Continuing from the synthesized research findings, it is clear that the application area of blockchain in healthcare AI is vast and multifaceted. The integration of blockchain technology is not limited to securing electronic health records but extends to enhancing the entire healthcare delivery system. This includes patient data management, drug traceability, clinical trials, and personalized medicine, where secure and transparent data handling is paramount. As the healthcare industry continues to innovate, blockchain and AI will likely expand into new areas, such as advanced biometrics for patient identification and decentralized autonomous organizations (DAOs) for patient-led research initiatives. To realize these advancements, stakeholders must address existing challenges through interdisciplinary collaboration, investment in technology infrastructure, and the development of regulatory frameworks that balance innovation with ethical considerations. Continuous dialogue between technologists, healthcare professionals, patients, and policymakers is essential to navigating the complexities of integrating these transformative technologies into healthcare. With a concerted effort, integrating blockchain and AI can lead to a more secure, efficient, and patient-centered healthcare system [18].

The convergence of blockchain and AI in healthcare applications presents a promising avenue for addressing data privacy and integrity challenges. Blockchain's attributes of decentralization, immutability, and transparency complement AI's capabilities, creating a secure environment for handling sensitive healthcare data. The studies by [14–17] collectively underscore the potential of blockchain technology in enhancing the security and efficiency of healthcare AI systems. As the healthcare industry continues to evolve with the integration of AI and blockchain, it is crucial to address the ongoing challenges and threats to data security. Continuous research and development are necessary to refine these technologies and their applications in healthcare. Future research directions may include optimizing blockchain and AI algorithms, developing more robust security measures, and exploring new application areas within the healthcare sector. Blockchain technology offers a robust framework for addressing AI's healthcare privacy and data integrity challenges. By leveraging the strengths of blockchain and AI, healthcare systems can achieve higher security and efficiency, ultimately leading to improved patient care and trust in digital healthcare services. The body of research discussed herein provides valuable insights and a solid foundation for future advancements in this interdisciplinary field.

3.3.2. Federated Learning: Enhancing Privacy in Healthcare AI

Federated Learning (FL) represents a paradigm shift in developing Artificial Intelligence (AI) models, particularly in sensitive healthcare. By enabling multiple institutions to collaborate on AI model development without exchanging patient data, FL addresses the most pressing concerns in healthcare AI: privacy and data integrity. Privacy is a fundamental concern when dealing with healthcare data due to its sensitive nature. Traditional machine learning approaches often require centralizing data from various sources, which poses significant privacy risks. FL circumvents this issue by allowing each participating institution to retain its data locally. As Ref. [19] explains, only the model parameters or gradients—essentially the learned features or updates to the model—are shared with a central server or among participants. This ensures that the raw patient data, which may contain personally identifiable information, never leaves the institution's premises where it was collected. Using techniques such as Secure Multi-party Computation (SMC) and Differential Privacy (DP) further enhances privacy in FL. SMC allows for the computation of functions across different inputs while keeping those inputs private, which is ideal for scenarios where data cannot be pooled together. DP provides a mathematical framework that guarantees that the outcome of an analysis is not significantly affected by the inclusion or exclusion of any individual's data. This means that even if someone had access to the output of a model trained with DP, they would not be able to infer much about any individual's data [13].

Data integrity is another critical challenge in healthcare AI. Data quality and consistency across different healthcare institutions can vary greatly, leading to biased or non-generalizable AI models. FL offers a solution to this by enabling the development of models that learn from a diverse and representative dataset. Since each institution trains a local model on its own data, the global model benefits from a wide range of data sources, leading to more accurate and robust AI models. These models are better equipped to perform well across different patient populations and healthcare settings, as they are not limited to data from a single source. Moreover, FL can help address the issue of data fragmentation in healthcare. As healthcare data are often siloed across various institutions, FL allows for connecting these fragmented data sources while maintaining privacy. This is particularly beneficial for tasks such as patient similarity learning, representation learning, and predictive modeling, where the ability to draw insights from a comprehensive dataset is crucial. By leveraging data from multiple institutions, FL can help create more accurate and generalizable models that reflect the global patient population, thus improving the quality of care [13].

Despite the advantages of FL in preserving privacy and ensuring data integrity, several challenges need to be addressed to fully realize its potential in healthcare AI. The authors

of [19] highlight the statistical variance in data distribution among clients, communication efficiency, and the potential for malicious clients as operational challenges in FL. The statistical heterogeneity of data across different institutions can lead to skewed models if not correctly managed. Communication efficiency becomes a concern when dealing with many participants, as the exchange of model updates can be bandwidth-intensive. Additionally, the risk of malicious clients attempting to compromise the model or infer sensitive information requires robust security mechanisms [13].

To address these challenges, future research in FL should focus on improving data quality, incorporating expert knowledge into the learning process, developing incentive mechanisms to encourage participation, and personalizing healthcare applications. Ensuring high-quality data are essential for the success of FL, as the models are only as good as the data they learn from. Expert knowledge can guide the learning process, making the models more practical and clinically relevant. Incentive mechanisms are necessary to motivate institutions to participate in FL, while personalization is critical to tailoring healthcare solutions to individual patient needs. Federated Learning holds significant promise for overcoming privacy and data integrity challenges in healthcare AI. FL can facilitate the development of robust, accurate, and generalizable AI models by enabling collaborative model training across various institutions while safeguarding data privacy. However, realizing the full potential of FL will require ongoing research to tackle operational challenges, improve data quality, and ensure the models are clinically relevant and personalized for patient care. As the healthcare industry continues to evolve, FL is a beacon of innovation, guiding the way toward more secure, efficient, and patient-centric AI solutions [13].

3.3.3. Unlocking Privacy: Harnessing Homomorphic Encryption for Healthcare AI

Homomorphic Encryption (HE) stands as a transformative technology in data security, particularly within the healthcare sector, where the confidentiality and integrity of patient information are of utmost importance. The ability of HE to enable computations on encrypted data without the need to decrypt it first offers a powerful tool for maintaining privacy while still allowing for the valuable analysis and utilization of healthcare data by Artificial Intelligence (AI) systems. The study by [20] delves into the intricacies of HE and its application in healthcare AI, providing a detailed exploration of how HE can address the twin challenges of privacy and data integrity. The authors elucidate the operational mechanisms of HE, the evolution of various HE schemes, and the practical considerations for its implementation in healthcare environments. One of the pivotal advantages of HE in healthcare AI is its role in cloud computing. As healthcare providers increasingly rely on cloud services for data storage and computation, the risk of exposing sensitive patient data to third-party service providers becomes a significant concern. HE mitigates this risk by ensuring that only encrypted data are processed by these external entities, thus maintaining the confidentiality of patient information even in a distributed computing environment [9].

The operational mechanism of HE is a multi-step process that begins with the encryption of data by the client before it is sent to the cloud service provider. The provider then performs the necessary computations on the encrypted data using HE techniques, which results in encrypted outputs. A notable challenge in this process is the accumulation of noise with each operation, which can degrade the quality of the encryption. Techniques such as bootstrapping and squashing are employed to manage this noise and maintain the integrity of the encrypted data. The client then decrypts the results, ensuring that the sensitive information remains secure. The authors of [20] also provide a historical perspective on the evolution of HE schemes, tracing back to the early concept of 'privacy homomorphism'. This foundational work laid the groundwork for subsequent developments in the field, including the Goldwasser-Micali and Elgamal schemes, which introduced improvements in security and functionality. The additive homomorphic method allowed for operations on encrypted text that corresponded to addition operations on plaintext, while the Paillier

cryptosystem expanded the capabilities of HE to include both addition and multiplication operations on encrypted data [9].

Despite the promising capabilities of HE, challenges still need to be fully addressed to harness its potential in healthcare AI. One of the primary challenges is the computational intensity associated with HE operations. The encryption and decryption processes and the computations on encrypted data are resource-intensive and can be significantly slower than operations on plaintext. This presents a hurdle for the real-time analysis and processing of large datasets commonly encountered in healthcare applications. Researchers are optimizing HE algorithms to improve efficiency and make them more practical for widespread use in healthcare AI. Another area of focus is the scalability of HE solutions. As healthcare systems generate vast amounts of data, the HE methods must be able to scale accordingly to handle the increasing volume while maintaining the same level of security and privacy. This requires advancements in the underlying cryptographic techniques and the infrastructure that supports HE, such as cloud computing platforms and specialized hardware [9].

Furthermore, the integration of HE into existing healthcare IT systems poses its own set of challenges. Healthcare providers must navigate the complexities of implementing HE within their current workflows, ensuring compatibility with existing software and hardware, and training staff to use the new systems effectively. The cost of adoption is also a consideration, as deploying HE solutions may require significant investment in technology and expertise. Despite these challenges, the benefits of HE in healthcare AI are clear. By enabling secure and private data analysis, HE facilitates the development of more accurate and personalized predictive models, which can lead to better patient outcomes. It also allows for secure data sharing between healthcare providers and researchers, fostering collaboration and innovation while protecting patient privacy. As the technology matures and solutions to the current challenges are found, HE is poised to play a critical role in the future of healthcare AI, offering a path to harness the power of data while upholding the highest standards of privacy and data integrity. As the healthcare industry continues to evolve with AI and cloud computing integration, HE will remain an essential tool for ensuring that patient data are handled with the utmost security and confidentiality, ultimately contributing to advancing healthcare technology and patient care [9].

3.3.4. Differential Privacy: Advanced Techniques in Healthcare AI

Differential Privacy (DP) is a critical privacy-preserving technique that has gained significant traction in healthcare AI due to its ability to provide strong privacy guarantees. It functions by introducing a calculated amount of random noise, either to the data itself or to the outputs of algorithms, thereby making it statistically challenging for attackers to deduce sensitive information about any individual in the dataset. This method is advantageous for sharing insights from health data, such as statistical summaries or AI model parameters, while safeguarding patient confidentiality. The core principle of DP is to ensure that the presence or absence of any individual's data do not substantially alter the outcome of an analysis. This feature is vital in healthcare settings where the sensitivity of patient data necessitates the utmost levels of confidentiality. DP's application extends to various algorithms, including but not limited to boosting, principal component analysis, support vector machines, and deep learning. It is also effectively employed in Federated Learning scenarios involving decentralized data processing across multiple entities, such as hospitals or research institutions, to prevent indirect data leakage—a prevalent issue in collaborative environments [19].

Despite its benefits, it is crucial to acknowledge that DP is inherently a 'lossy' technique. While it excels at enhancing privacy, it can simultaneously lead to reduced accuracy of predictions or analyses due to the added noise. This inherent trade-off between privacy and utility is a pivotal consideration in the deployment of DP within healthcare AI. As privacy protection intensifies with increased noise, the usefulness of the data for research and the accuracy of AI models may be compromised. To counterbalance this, researchers

often integrate DP with other methods like Secure Multi-party Computation (SMC) to balance privacy and data utility [19]. This hybrid approach is designed to control the escalation of noise with the number of participants, thus maintaining both privacy and the practical value of the data. DP presents a robust framework for preserving individual privacy in healthcare AI applications, particularly in distributed data processing contexts. Its capability to prevent data leakage must be carefully weighed against the potential diminution in prediction accuracy and data utility. Therefore, meticulous implementation and, where necessary, incorporating additional privacy-preserving techniques are essential to optimizing the benefits of DP in healthcare AI [10].

3.4. Ethical Technologies as Cornerstones in Healthcare AI

Integrating blockchain, Federated Learning (FL), Homomorphic Encryption, and Differential Privacy into healthcare AI systems is a multifaceted endeavor that addresses the pressing need for ethical standards and the protection of patient rights in the rapidly evolving field of healthcare technology. Collectively, these technologies form a robust framework for managing the challenges associated with the privacy and security of sensitive healthcare data while fostering innovation and efficiency in healthcare delivery.

Blockchain technology stands out for its unique attributes of decentralization, immutability, and transparency, which are particularly beneficial in the context of healthcare AI systems. By creating a secure and tamper-proof ledger for medical data transactions, blockchain technology ensures the integrity and traceability of patient data, which is paramount in clinical settings. For instance, blockchain can be used to securely manage electronic health records (EHRs), providing a reliable source of patient data for healthcare professionals and AI algorithms while preventing unauthorized access and data breaches [19]. Federated Learning (FL) represents a paradigm shift in data analysis and machine learning, particularly within the healthcare sector. By enabling the training of AI models on decentralized data sources, FL ensures that sensitive patient information remains within the confines of the local institution, thereby preserving privacy. This approach is crucial for predicting hospital readmission risks and screening for medical conditions using wearable device data. FL's ability to integrate data from various sources without compromising privacy is a testament to its potential to enhance the capabilities of healthcare AI systems. Homomorphic Encryption is a cryptographic technique that allows computations to be performed on encrypted data without the need to decrypt it first. Healthcare providers can analyze and process sensitive patient data while it remains encrypted, significantly reducing the risk of data exposure. Homomorphic Encryption in healthcare AI systems enables secure data utilization, ensuring patient confidentiality is maintained even during complex data analysis processes [15]. Differential Privacy is a technique that adds a certain amount of noise to data queries, making it difficult to identify individual records while allowing for accurate aggregate analysis. This approach is particularly relevant in healthcare, where patient data are susceptible. Differential Privacy ensures that the privacy of individual patients is not compromised when their data are used for research or to train AI models. By integrating Differential Privacy into healthcare AI systems, researchers and clinicians can gain valuable insights from large datasets without risking the exposure of personal health information, thus maintaining patients' trust and complying with stringent privacy regulations such as GDPR and HIPAA [21].

The Internet of Healthcare Things (IoHT) represents a significant advancement in healthcare data management, with devices such as smartwatches and wearable trackers collecting a wealth of health-related data. These data are invaluable for healthcare professionals to make informed decisions regarding disease treatment and management. However, the traditional centralized machine learning models face challenges related to data access restrictions, potential biases, and high resource demands. Integrating blockchain, FL, Homomorphic Encryption, and Differential Privacy within IoHT systems offers solutions to these challenges, ensuring that data are managed ethically and securely while enabling innovative healthcare solutions [15]. Despite the promise of FL, there are inherent chal-

lenges, such as the statistical diversity of data across clients and communication efficiency. Techniques like Agnostic Federated Learning and q-Fair Federated Learning have been proposed to address the issue of data heterogeneity. At the same time, client selection protocols, model compression, and update reduction strategies aim to improve communication efficiency. Moreover, integrating Secure Multi-party Computation and Differential Privacy within FL frameworks enhances the privacy and security of the data, making FL a powerful tool for healthcare applications [19].

As AI continues to reshape healthcare, integrating blockchain, FL, Homomorphic Encryption, and Differential Privacy is critical for addressing the complex challenges of intelligent healthcare systems. These technologies enhance the security and privacy of healthcare delivery and ensure that ethical standards are upheld. The collective application of these technologies represents a vision for a future where healthcare AI advances in tandem with ethical considerations, with patient welfare remaining at the core of technological progress [21]. The detailed integration of blockchain, Federated Learning, Homomorphic Encryption, and Differential Privacy into healthcare AI systems is a testament to the commitment to ethical standards and the protection of patient rights. These technologies address the technical challenges of privacy and data security, encapsulating a dedication to respecting and protecting patient autonomy. As the healthcare industry continues to innovate, the role of these technologies in maintaining a balance between innovation and ethical responsibility is vital. They offer solutions for a future where the advancement of healthcare AI occurs hand-in-hand with safeguarding patient welfare, ensuring that the benefits of technology do not come at the expense of privacy and trust.

Integrating these advanced technologies into healthcare AI systems is not merely a technical exercise but a patient-centric approach that prioritizes the well-being and rights of individuals. By leveraging blockchain, healthcare providers can offer a more transparent and patient-controlled exchange of medical data, empowering patients to have a say in who accesses their information. Federated Learning enables the development of more personalized treatment plans by analyzing data from a diverse patient population while keeping individual data localized and private. Homomorphic Encryption and Differential Privacy further contribute to this patient-centric approach by allowing for the secure and private analysis of health data, ensuring that patients' identities are shielded from potential misuse [15]. The healthcare sector is heavily regulated to protect patient information and ensure the ethical use of data. The technologies discussed herein play a crucial role in helping healthcare organizations navigate the complex landscape of regulatory compliance. By adopting these technologies, healthcare providers can meet the requirements of laws such as HIPAA in the United States and GDPR in Europe, which mandate strict data privacy and security standards. The ethical considerations of patient data use are also addressed, as these technologies provide mechanisms to ensure that patient consent is obtained and that data are used to respect individual autonomy and dignity [19].

Integrating blockchain, FL, Homomorphic Encryption, and Differential Privacy into healthcare AI systems requires collaborative efforts across various disciplines, including computer science, healthcare, law, and ethics. Interdisciplinary teams must work together to design systems that are both technologically sound, ethically responsible, and legally compliant. This collaboration is essential for creating healthcare AI systems trusted by patients, clinicians, and society. While the potential of these technologies is immense, there are still challenges to be addressed, such as ensuring data quality, incorporating expert knowledge into AI models, designing efficient incentive mechanisms for data sharing, and improving the precision of AI algorithms. Addressing these challenges will require ongoing research, innovation, and a commitment to continuous improvement. As the healthcare industry moves forward, these technologies must evolve to meet the ever-changing needs of healthcare delivery and the expectations of patients. Ensuring data quality is critical, as the efficacy of AI models heavily depends on the input data's accuracy and reliability. Involving medical experts in the training process is equally essential to providing domain-specific insights that can enhance the performance and relevance of AI algorithms [21].

Designing efficient incentive mechanisms is another area that requires attention. These mechanisms are necessary to encourage the sharing of data among institutions and individuals, which is fundamental for the success of Federated Learning [9]. Without proper incentives, the potential of collaborative AI model training may not be fully realized. The personalization of healthcare through AI also presents both a challenge and an opportunity. As AI systems become more sophisticated, they can be tailored to individual patient needs, leading to more effective and personalized treatment plans. However, achieving this level of personalization requires a deep understanding of individual patient data and the ability to adapt AI models accordingly. Finally, improving the precision of AI models in healthcare is an ongoing pursuit. As models become more accurate, they can provide better predictions and recommendations, improving patient outcomes. However, this requires a careful balance between model complexity and interpretability, ensuring that healthcare professionals can understand and trust the AI-driven decisions [5].

As we look to the future, the ethical imperative for developing and integrating AI in healthcare remains paramount. The technologies of blockchain, Federated Learning, Homomorphic Encryption, and Differential Privacy offer a framework for ethical AI by prioritizing the privacy, security, and autonomy of patient data. These technologies must be developed and implemented with a clear ethical vision that places patients' well-being above all else. Integrating blockchain, Federated Learning, Homomorphic Encryption, and Differential Privacy into healthcare AI systems is a complex but necessary step toward a more secure, private, and ethical healthcare landscape [9]. These technologies provide the tools needed to navigate the challenges of data security and patient privacy in an increasingly digital world. As AI continues to transform healthcare, the commitment to ethical standards and the protection of patient rights must remain at the forefront of technological advancements. The future of healthcare AI is not just about harnessing the power of data but doing so in a way that respects and enhances the human element of healthcare. With continued research, collaboration, and ethical vigilance, the integration of these technologies will lead to a healthcare system that is more efficient, effective, and more aligned with society's values [5].

The ongoing dialogue between technology developers, healthcare providers, policy-makers, and patients is crucial to ensuring that the deployment of AI in healthcare reflects a collective vision that values privacy, security, and ethical responsibility. As these stakeholders engage in this conversation, it is essential to consider the broader implications of technology on accessibility, equity, and the potential for disparities in healthcare outcomes. The promise of AI in healthcare must be accessible to all population segments. This includes ensuring underserved communities have the same opportunities to benefit from AI-driven healthcare advancements. Equity in healthcare AI also means that algorithms are free from biases that could perpetuate disparities in health outcomes. Integrating blockchain, FL, Homomorphic Encryption, and Differential Privacy can help mitigate these risks by providing a secure and unbiased data analysis framework [9].

Research and development efforts must continue to improve the technologies underpinning healthcare AI systems. This includes enhancing the scalability of blockchain, the efficiency of Federated Learning algorithms, the performance of Homomorphic Encryption techniques, and the effectiveness of Differential Privacy measures. Additionally, interdisciplinary research can explore new ways to integrate these technologies, creating even more robust solutions for healthcare data management. As technology evolves, so must the regulatory frameworks governing its use. Regulators must stay abreast of technological advancements to ensure that laws and guidelines protect patient data and promote ethical AI practices. This may involve updating existing regulations or creating new ones that address the unique challenges posed by integrating blockchain, FL, Homomorphic Encryption, and Differential Privacy in healthcare. The journey towards integrating advanced technologies into healthcare AI systems is ongoing and requires a concerted effort from all stakeholders. The potential benefits are vast, including improved patient outcomes, enhanced privacy and security, and a healthcare system that is more responsive to the needs of all individuals.

By maintaining a focus on ethical standards, patient rights, and societal values, the future of AI in healthcare cannot only leverage the power of data but also embody the principles of compassion, fairness, and respect for human dignity [5,9,21].

The complexity of integrating blockchain, FL, Homomorphic Encryption, and Differential Privacy into healthcare AI systems suggests that public-private partnerships could play a significant role. Collaboration between government agencies, technology companies, healthcare institutions, and academic researchers can accelerate innovation, share risks, and pool resources to tackle the challenges associated with these technologies. As AI becomes more ingrained in healthcare, there is a growing need for ethical AI governance structures. These structures should oversee the development and deployment of AI systems, ensuring that they adhere to ethical guidelines and that there is accountability for their impact on patients and society. This governance could be internal ethics boards within organizations, industry-wide consortia, or independent oversight bodies [9,21].

Patients must actively participate in conversations about how their data are used in healthcare AI. Engaging with patients to understand their concerns and preferences can lead to better-designed AI systems that respect patient autonomy and promote empowerment. Education and awareness are critical components in the successful integration of these technologies. Healthcare professionals must be educated about the capabilities and limitations of AI systems, and patients must be informed about how their data are being used and protected. This transparency is essential for building trust and ensuring all parties are comfortable using AI in healthcare. Blockchain can facilitate patient engagement by giving individuals control over their health data and who can access it. Integrating blockchain, Federated Learning, Homomorphic Encryption, and Differential Privacy into healthcare AI systems is a complex but necessary endeavor to ensure that the digital transformation of healthcare is conducted ethically and responsibly. It requires a collaborative, interdisciplinary approach that balances technological innovation with protecting patient rights and societal values. As we move forward, it is crucial to continue exploring and addressing the technical, ethical, and regulatory challenges that arise to create a healthcare system that is not only intelligent but also just and equitable for all [9,21].

3.5. Algorithmic Fairness, Transparency, and Trust in AI-Driven Healthcare

In AI-driven healthcare, a multifaceted approach is vital to ensure algorithmic fairness, transparency, and trust, which are pivotal for equitable and ethical healthcare delivery. Mitigating algorithmic bias is crucial for equitable patient treatment and involves analyzing and adjusting AI models to reflect diverse patient demographics. Including diverse datasets in AI model training is essential for minimizing biases and promoting equitable health outcomes [8,22]. Additionally, AI fairness and bias detection tools are essential for analyzing and readjusting algorithms to ensure fair treatment across patient demographics. Developing transparent and understandable AI systems is critical to building trust among healthcare stakeholders, addressing the nature of AI algorithms' 'black box' nature, and improving the understanding of AI processes [2,23]. Explainable AI (XAI) plays a foundational role in making AI decisions and processes more comprehensible, thus enhancing transparency and fostering trust. This comprehensive methodology ensures that AI applications cater effectively to the diverse needs of patient populations and establishes a trust-based relationship between AI applications and healthcare users, ensuring AI's role remains informative and supportive [13].

Incorporating fairness and explanation in AI-informed healthcare decision-making, as noted by [24], is paramount to ensuring ethical AI integration. AI systems must refrain from perpetuating or introducing new forms of discrimination, especially given the diversity of patient populations. Detecting and mitigating biases in AI models is essential for equitable treatment across all patient groups. The development of AI models that are both fair and explainable allows healthcare providers and patients to understand and trust AI decisions, reinforcing patient autonomy and agency. Moreover, integrating AI into healthcare demands attention to patient dignity and respect. The authors of [25] explore

how AI perceptions in healthcare are tied to how these systems uphold human dignity, highlighting the need for AI applications to respect patient values. This aligns with broader ethical considerations in healthcare AI, particularly concerning patient autonomy, data privacy, and algorithmic bias. In the broader context of AI decision-making, [26] points out the risk of AI simplifying patient narratives, emphasizing the need for AI systems to augment personalized care while maintaining essential human elements for adequate healthcare. The authors of [27] emphasize patient engagement, advocating for informed and active involvement in AI-related healthcare decisions. Addressing algorithmic discrimination, enhancing transparency, and fostering trust in AI applications are crucial for ethical and patient-centered healthcare. Adopting frameworks that emphasize fairness, transparency, and explanation, alongside a focus on human dignity and patient engagement, AI in healthcare can achieve more equitable and trustworthy outcomes, aligning technological innovation with ethical considerations.

Integrating the AI-driven Internet of Things (AIoT) in healthcare presents unique challenges and opportunities for ensuring algorithmic fairness, transparency, and trust. Mitigating bias in AI algorithms is paramount, especially considering the diverse nature of patient populations and the varied nature of diseases and conditions. The research by [21] highlights the rapid adoption of AIoT in healthcare, significantly enhancing the quality and effectiveness of healthcare services. This adoption is particularly valuable for chronic conditions, elderly care, and continuous monitoring. Incorporating diverse data sets into AI model training minimizes biases and promotes equitable health outcomes. The use of AIoT, including remote monitoring and communication, significantly enhances patient treatments. Mobile medical applications and wearable devices enable patients to capture personal health data, empowering them to actively manage their health. This approach aligns with the need for diverse data sets, capturing a wide range of patient data and leading to more personalized and effective healthcare solutions.

The importance of reducing medical errors through AI-driven decision-support systems cannot be overstated. AIoT has evolved to use complex algorithms like neural networks, decision trees, and support vector machines, which are instrumental in making health-related decisions more effectively. These technologies, however, must be developed with fairness in mind, ensuring they do not perpetuate existing biases or create new ones. Security and privacy are critical concerns in the AIoT framework. The emphasis is placed on the need for well-defined architecture standards, including interfaces, data models, and relevant protocols, to support a variety of devices and languages. Identity management within the Internet of Things is crucial to solving both security and privacy risks associated with AIoT. This involves exchanging identifying information between devices and employing cryptography and other techniques to prevent identity theft. Ensuring algorithmic fairness, transparency, and trust in AI-driven healthcare necessitates focusing on diverse data sets and fairness tools. This approach contributes to equitable patient treatment and outcomes by enhancing personalized care and reducing medical errors. Additionally, addressing security and privacy challenges in AIoT is essential for successfully implementing and scaling up these technologies in healthcare. Implementing a proper governance framework across various aspects of AIoT architecture and standardization is crucial for realizing the full potential of AI in transforming healthcare [22].

The control and sharing of healthcare data have been central to discussions about AI in healthcare. It is emphasized that the flow of data towards AI is crucial, with arguments against approaches that restrict this flow. Such restrictions could hinder the development of future AI applications and diminish the need for data to train them. They suggest that existing experiences in monetizing digitalized content, such as music, offer a practical solution to incentivize patients to share their data without restricting data flows. The AI market's dominance by a few mega-firms necessitates policies that allow individuals to control their data and represent their interests collectively. The article outlines various initiatives, like the Health Data Hub, SOLID, and DECODE, which aim to control data flow and induce artificial scarcity. However, this may not apply to AI, as AI is 'data-hungry'.

Less data lead to fewer AI applications, thus limiting the demand for data to train and furnish these applications [8].

AI's reliance on data underscores the need for organized markets to facilitate data flow toward AI. However, transaction costs associated with data trade often exceed the value of the exchange itself, making the negotiation and licensing of data unprofitable. Thus, agents must bargain for some indemnification directly with AI firms. Attention is suggested to be shifted towards methods that allow for unrestricted data flows, which is vital for ensuring algorithmic fairness, transparency, and trust. The concept of Collective Data Management (CDM) is introduced as a means to enable firms to accumulate, process, utilize, and benefit from data while jointly overseeing data usage and negotiating some form of ex-post compensation. Drawing from the experiences of Collective Rights Management (CRM), this approach seeks to establish transparency and accountability in data governance, thereby nurturing public trust and confidence [8].

The integration of CDM into the legal framework is crucial for its success. The technical infrastructure of CDM must respect data governance processes designed to achieve transparency, integrity, security, and accountability. This is vital for acknowledging the social relationship created by using healthcare data, which entails responsibility and awareness of how data use aligns with societal values. Such governance is essential in fostering a trust-based relationship between AI applications and healthcare users, ensuring AI's role remains informative and supportive. Adopting frameworks emphasizing fairness, transparency, and explanation in AI-informed healthcare decision-making is paramount. Such frameworks must be grounded in existing legal practices and adapted to new challenges in data management, ensuring that technological innovation aligns with ethical considerations for equitable and trustworthy outcomes in healthcare. The concept of CDM, as proposed by [8], offers a pathway to balance the need for data to fuel AI development with the rights of individuals to control and benefit from their data. This balance is critical to maintaining the integrity of healthcare data and the trust of those it serves. Furthermore, the integration of AIoT in healthcare, as highlighted by [21], underscores the importance of a robust governance framework that addresses algorithmic fairness and ensures patient data security and privacy. Developing fair, transparent, and trustworthy AI applications requires a concerted effort to standardize AIoT architecture, promote diverse datasets, and implement fairness tools that can detect and mitigate biases. The future of AI-driven healthcare hinges on the ability to create systems that are not only technologically advanced but also ethically sound and socially responsible. By fostering algorithmic fairness, ensuring transparency, and building trust through explainability and data governance, AI can significantly enhance healthcare delivery while respecting the dignity and autonomy of patients. AI will become a supportive and informative ally in pursuing better health outcomes for all through these efforts.

3.6. Legal and Regulatory Considerations

Integrating Artificial Intelligence (AI) in healthcare, while offering transformative potential, necessitates a rigorous alignment with ethical standards and medical ethics principles to ensure patient welfare and equitable access. The legal and ethical challenges, particularly concerning data privacy and patient consent, are highlighted by the authors of [28], who stress the importance of robust legal frameworks that are adaptable and responsive to the evolving nature of AI applications. These frameworks must harmonize with regulations such as the General Data Protection Regulation (GDPR) to ensure ethical AI usage in healthcare. The incorporation of blockchain technology in AI-driven healthcare, as explored by [29], adds another layer of complexity to these challenges. Blockchain offers opportunities for enhancing data security and patient privacy but also challenges aligning with GDPR requirements. Specialized regulatory guidance tailored to blockchain applications in healthcare is necessary to address blockchain's technical intricacies and ensure ethical and legal compliance. Furthermore, private entities' control of health data in the AI commercial sector, as exemplified by the DeepMind-Royal Free London NHS Foun-

dation Trust case, underscores the need for dynamic and adaptable legal and regulatory frameworks. These frameworks must safeguard patient interests and ensure responsible AI utilization in healthcare [1]. The intersection of blockchain technology with GDPR in AI-driven healthcare requires a comprehensive approach encompassing technological adaptability, ethical considerations, and the development of responsive legal frameworks.

Integrating Artificial Intelligence (AI) in healthcare necessitates a multifaceted approach to uphold ethical standards and protect patient welfare. To navigate the complexities of privacy and data security, it is imperative to implement rigorous data protection measures, ensuring AI technologies conform to the highest standards through advanced data anonymization and encryption techniques. Private entities' governance of patient data access, usage, and control demands clear guidelines and oversight, addressing the inherent risks of AI, such as errors, biases, and the opacity of algorithmic decision-making processes. To counter the risks of privacy breaches and the potential reidentification of individuals from anonymized datasets, healthcare systems must fortify their defenses with sophisticated computational strategies and ongoing risk assessments [1,28].

Addressing the legal and regulatory challenges involves drafting comprehensive contracts that clearly define the rights and obligations of all stakeholders in AI healthcare initiatives, with regulations mandating that patient data remain within its original jurisdiction except under specific conditions. The exploration of generative models to create synthetic patient data emerges as a promising solution to privacy concerns, enabling the advancement of machine learning without relying on actual patient data. A strong emphasis on patient agency and informed consent is also critical, ensuring transparent communication regarding data withdrawal rights and the necessity for repeated consent for new data applications. As AI technology rapidly evolves, regulatory innovation is essential to keep pace. This includes developing new data protection methods and a regulatory framework that mandates private data custodians to utilize cutting-edge and secure data privacy practices. By embedding these measures within the legal and regulatory frameworks that govern AI in healthcare, we can maintain patient and public trust, respect patient dignity and autonomy, and adhere to medical ethics principles. Such an environment is conducive to the responsible development and application of AI, enabling healthcare systems to harness AI's potential to improve patient outcomes, increase care efficiency, and provide equitable access to state-of-the-art medical technology [1,28,29].

3.7. *Balancing Innovation with Ethical Standards*

Integrating Artificial Intelligence (AI) necessitates a critical balance between technological innovation and adherence to ethical standards in the rapidly evolving healthcare field. This equilibrium is essential as the healthcare sector seeks to leverage AI's potential to enhance patient outcomes significantly. The ethical integration of AI in healthcare demands a commitment to the core principles of medical ethics: beneficence, non-maleficence, autonomy, and justice. These principles dictate that AI applications must prioritize patient welfare and avoid harm, supporting patient decision-making and providing comprehensive, unbiased information while respecting the patient's right to informed choice. Justice in AI deployment requires equitable access to healthcare and the prevention of biases that might lead to treatment disparities. Moreover, as AI becomes more prevalent in healthcare, it is vital to mitigate the risk of dehumanizing patient care. AI should enhance, not replace, the human elements of empathy and understanding in patient care. Active patient involvement in AI-related healthcare decisions fosters a sense of agency and empowerment for patient satisfaction and trust in the healthcare system. Concurrently, evolving legal and regulatory frameworks governing AI's use in healthcare must address unique challenges such as data privacy, patient consent, and liability issues, ensuring AI technologies' safe and compliant deployment in healthcare [1,2,27]. The healthcare sector's journey toward integrating AI must be marked by a harmonious blend of innovation and ethical responsibility, ensuring that technological advancements in patient care align with patient dignity, rights, and well-being.

4. Advancing Data Integrity and Security in Healthcare AI: A Focused Approach to Blockchain and Advanced Data Validation Algorithms

4.1. In-Depth Analysis of Data Integrity in AI Healthcare Applications

The importance of maintaining data integrity and security in AI healthcare applications cannot be overstated. This is because it directly impacts patient safety and the effectiveness of healthcare delivery. Highlighting this [5] underscores the crucial nature of AI's impact on healthcare. Additionally, the authors of [7,8] emphasize the essential role of data integrity in ensuring reliable healthcare outcomes. They advocate for rigorous verification and validation mechanisms, which gain particular significance in precision-critical fields like ophthalmology, as noted in [30]. The importance of robust data management practices is further stressed by [31]. These practices include continuous monitoring for anomalies to uphold the integrity of health data. The seamless transition from robust data management to addressing patient data access and control challenges is crucial. These challenges, especially when data are private, underscore the need for robust regulatory frameworks and systemic oversight. This transition highlights the interdependence of data integrity and privacy, emphasizing how effective data management addresses access and control challenges. Moreover, the risks of reidentification in anonymized data require enhanced privacy and security measures to protect patient data against computational strategies capable of reidentifying individuals. This concern naturally leads us to the broader implications for patient trust and the ethical application of AI in healthcare, as argued by the authors [1,9,10].

The evolving nature of large language models (LLMs) like GPT-4 underscores the importance of addressing the scale and complexity inherent in these systems to maintain data integrity. The reliance of these models on extensive datasets and their potential for complex output generation necessitate enhanced data privacy and security measures, as well as robust verification and validation mechanisms. This point relates to the need for transparent and responsible AI usage in healthcare, which is a crucial factor in maintaining public trust. Lastly, the importance of technologically facilitated recurrent informed consent is underscored, which also mentions the dynamic regulatory approach as essential for ongoing data integrity and security in healthcare AI applications. This approach is critical in adapting to the ever-evolving landscape of AI technology, ensuring that as AI systems become more complex, the mechanisms to safeguard data integrity and privacy evolve alongside them [1,27].

The authors of [9] focus on the practicalities of ensuring data integrity in AI healthcare. It stresses the importance of maintaining the confidentiality and integrity of patient data, which is fundamental for developing reliable healthcare AI systems. The significant barrier to secure data access and usage at the commercial level is acknowledged. Privacy-Preserving Machine Learning (PPML) emerges as a key solution, enhancing data and machine learning security—a vital step in overcoming these barriers. Particularly in sensitive datasets, which are integral to developing life-saving treatments and making critical decisions, PPML methods allow for collaborative training of ML models without compromising private information's unique structure. This method safeguards patient data and facilitates the responsible development and application of AI in healthcare settings.

4.2. Technologies for Assuring Data Integrity in Healthcare AI

Integrating advanced technologies such as Homomorphic Encryption (HE), Differential Privacy (DP), and blockchain technology is innovative and essential in addressing the complex data security challenges in AI-driven healthcare systems. As digital healthcare data proliferates at an unprecedented rate, the need for robust, sophisticated security mechanisms becomes ever more critical. These technologies offer more than just layers of security; they redefine how data can be safely used and shared in healthcare environments, ensuring that the integrity and reliability of sensitive health data are maintained. This is vital for safeguarding patient privacy, accurate and effective patient care, and medical research. By enhancing data confidentiality, ensuring anonymity, and preserving data

integrity, these technologies collectively form the backbone of secure, efficient, and trustworthy AI-driven healthcare systems, impacting everything from patient diagnosis to treatment outcomes [9].

The article by [9] provides a meticulous examination of the critical role played by Homomorphic Encryption (HE), Differential Privacy (DP), and blockchain technology in strengthening the privacy and security of AI-driven healthcare systems. The article navigates through the intricacies of HE, a cryptographic method that enables the performance of calculations on encrypted data without compromising its security, highlighting its utility in sensitive applications such as genomic data analysis, where patient privacy is paramount. It discusses state-of-the-art HE algorithms like DeCrypt that bolster security against specific cyber threats. It contemplates HE's potential to facilitate secure data analysis by authorized entities, fostering collaborative research while safeguarding patient confidentiality. The article further scrutinizes DP, a technique that injects a controlled amount of noise into data to protect individual privacy yet permits valuable aggregate analysis—balancing data utility against the imperative of protecting health information. It showcases the application of DP in various healthcare contexts, illustrating how it empowers researchers to extract insights from health data without compromising individual identities. Moreover, the article underscores the transformative impact of blockchain technology in healthcare, detailing its secure, immutable, and transparent transaction recording capabilities. It accentuates blockchain's decentralized nature, which ensures the integrity of medical records through a distributed ledger system that resists unauthorized alterations. This technology is lauded for its potential to enhance the accuracy and legal compliance of medical records, streamline health record management, curtail administrative costs, and improve the traceability of medical supplies. Collectively, these technologies are presented as a robust framework for ensuring data integrity and preventing unauthorized access, thereby shaping a more secure, efficient, and trustworthy healthcare system. This article is a key resource for grasping how privacy-preserving technologies are integrated into healthcare, underscoring their essential role in advancing digital healthcare and safeguarding sensitive patient information.

Together, these technologies enhance data confidentiality, preserve data integrity, and ensure anonymity in AI-driven healthcare systems. They enable the secure use and sharing of sensitive health data, critical for patient privacy, accurate patient care, and medical research. The article emphasizes the significance of these technologies in transforming healthcare systems, making them more secure, efficient, and trustworthy. This transformation profoundly impacts various aspects of healthcare, from patient diagnosis to treatment outcomes, and even extends to the broader realm of public health and epidemiology. The article by [9] thoroughly explores the role of HE, DP, and blockchain in overcoming privacy and security challenges in AI-based healthcare systems. It presents these technologies as a robust framework for safeguarding patient data, essential for modern healthcare systems' effective and secure operation. Integrating these technologies is a critical step toward realizing a new paradigm in healthcare, where data-driven insights and AI-powered solutions can be leveraged to their fullest potential while upholding the highest data privacy and security standards. The article is a comprehensive resource for understanding privacy-preserving technologies' current state and future potential in the healthcare industry.

4.2.1. Homomorphic Encryption (HE): Enhancing Data Confidentiality

Homomorphic Encryption (HE) is transformative in securing sensitive healthcare data. By enabling computations on encrypted data, HE ensures data confidentiality even during processing. This feature is critical when handling sensitive information such as genomic data, which forms the cornerstone of precision medicine and other advanced medical research. With its complex and personal nature, genomic data demand stringent privacy measures. HE meets this demand by allowing data owners to encrypt their data before sending it for computation, thus ensuring that sensitive information remains confidential throughout the process. The computational tasks are performed on this encrypted data

without decryption, preserving data attributes and ensuring that third parties can process it without accessing its original, unencrypted form. This aspect of HE is particularly beneficial in scenarios where data need to be shared among multiple researchers or institutions. It provides a secure way to collaborate and gain insights from sensitive data without compromising privacy, thus fostering a more collaborative and productive healthcare research environment [9].

Building upon this understanding, the analysis by [20] delves into the multifaceted significance of HE in healthcare, particularly in the context of cloud computing and cloud storage. Traditional encryption methods, which decrypt data before processing, risk exposing sensitive medical information. HE circumvents this risk by allowing computations on encrypted data, thereby maintaining the confidentiality of sensitive patient information, such as genomic data, throughout the processing phase. This is especially pertinent for genomic data, which are integral to precision medicine and advanced medical research. By encrypting this data prior to computation, HE ensures privacy preservation, even when third parties are involved in handling the data. The increasing adoption of cloud computing in healthcare amplifies the need to protect patient-sensitive data. HE addresses this need by enabling data processing in an encrypted form, ensuring that service providers only have access to encrypted data, thereby maintaining privacy and confidentiality. This is a critical consideration in healthcare environments where data are frequently shared across various platforms and institutions, and robust encryption methods are required to prevent unauthorized access. Moreover, HE is pivotal in collaborative healthcare research and data sharing. It allows for the secure sharing of sensitive data among multiple researchers or institutions without compromising privacy. This capability is essential for collaborative healthcare research, where gaining insights from sensitive data is necessary but must be carried out without revealing the actual data. The ability to perform computations on encrypted data enables a secure and productive exchange of information, which advances medical research while adhering to strict privacy standards.

The evolution of HE has introduced various schemes, each with its own capabilities and limitations. Starting with Partial Homomorphic Encryption (PHE), which supports limited operations, the field has progressed to Somewhat Homomorphic Encryption (SWHE) schemes that allow for an arbitrary number of operations but are constrained by noise generation. The advent of Fully Homomorphic Encryption (FHE) marked a significant breakthrough by supporting an unlimited number of operations on encrypted data. Despite this advancement, FHE still grapples with noise management challenges, necessitating bootstrapping and squashing techniques to maintain the integrity of the encryption. The technological underpinnings of advanced HE schemes are often based on the lattice-based approach, including Learning with Errors (LWE). The difficulty of solving lattice problems, which LWE is predicated upon, provides a strong foundation for cryptography, particularly in healthcare scenarios where data security is paramount. The robustness of LWE-based schemes is further underscored by their potential resistance to quantum computing attacks, making them a viable option for post-quantum cryptography and ensuring the long-term security of healthcare data [20].

Enhancing data confidentiality with HE involves integrating it into existing data management and analysis workflows. This integration requires the development of specialized algorithms capable of operating on encrypted data and optimizing encryption schemes to minimize computational overhead. The objective is to balance maintaining high security standards with achieving operational efficiency, allowing healthcare providers to adopt it without incurring significant performance drawbacks. HE also addresses regulatory compliance and ethical considerations in healthcare. For instance, the Health Insurance Portability and Accountability Act (HIPAA) in the United States mandates the protection of patient health information. HE can assist healthcare organizations in meeting these regulatory requirements by providing a secure method for handling and analyzing patient data. Furthermore, HE supports the ethical imperative of maintaining patient confidentiality, a cornerstone of patient trust and ethical medical practice [20].

Despite its promising potential, HE faces computational efficiency and implementation complexity challenges. Ongoing research is dedicated to optimizing HE schemes to enhance their practicality for real-world applications. Efforts include reducing the computational resources needed for encryption and decryption processes and simplifying HE integration with existing healthcare IT systems. As the technology continues to mature, HE is anticipated to become more accessible and widely adopted within the healthcare industry, leading to improved data security and privacy in an increasingly data-centric landscape. The application of HE in healthcare offers a secure means to handle sensitive patient data, particularly in cloud computing environments. Its ability to enable computations on encrypted data without exposing the actual data underlines its critical role in preserving privacy and fostering collaborative research. The evolving nature of HE, from PHE to FHE, and its reliance on advanced cryptographic concepts like LWE highlight its complexity and the ongoing efforts to optimize its efficiency and applicability in healthcare. As technology advances, it promises to transform how sensitive healthcare data are managed, shared, and analyzed while ensuring confidentiality and compliance with regulatory standards. The future of HE in healthcare looks promising as it stands at the intersection of technological innovation and the increasing demand for data privacy. The integration of HE into healthcare systems is expected to revolutionize data sharing and analysis, enabling new forms of secure data collaboration without compromising the privacy of individuals. As researchers and practitioners continue to address the challenges and refine the technology, HE is poised to become an indispensable tool in protecting sensitive healthcare information, ultimately contributing to advancing global health outcomes [20].

4.2.2. Differential Privacy: Ensuring Anonymity in Data Analysis

Differential Privacy (DP) has become an indispensable tool in the realm of healthcare data analysis, offering a robust solution to the perennial challenge of maintaining patient confidentiality while still allowing for the extraction of valuable insights from large datasets. The integration of DP into healthcare research is not merely a technical improvement but a fundamental shift in how patient data are handled, ensuring that the privacy of individual patients is safeguarded even as their data contributes to broader public health initiatives. This technology strikes a delicate balance between data utility and privacy, a balance that is essential for fostering patient trust and encouraging the sharing of data for research purposes. The application of DP in healthcare is particularly critical given the highly sensitive nature of medical information, where the unauthorized disclosure of personal health data can have profound implications for individuals' privacy and well-being [9].

Recent advancements in DP have been particularly focused on its synergy with machine learning models, especially in the context of Federated Learning (FL). FL represents a paradigm shift in model training, where multiple healthcare institutions can collaborate on model development without the need to exchange raw patient data, thereby preserving privacy at the source. However, FL is not immune to privacy breaches, and DP addresses this vulnerability by injecting controlled noise into the data or model updates. This ensures that the contributions of individual patients to the model are obfuscated, making it exceedingly difficult to trace back to any specific individual, as highlighted by [9]. The integration of DP with FL and blockchain, as discussed in the article, underscores the multifaceted approach to privacy preservation in healthcare, where DP is a central component in a suite of Privacy-Enhancing Technologies.

The trade-off between privacy and data utility is a central challenge in the application of DP, particularly in healthcare, where the stakes are high. The addition of noise to protect privacy can, paradoxically, diminish the quality of the data, potentially leading to less accurate models. This is a significant concern in healthcare, where the accuracy of predictions can have life-altering consequences. Researchers are actively engaged in finding the optimal balance, seeking to maintain high data utility while providing strong privacy guarantees, a pursuit that is at the forefront of Privacy-Preserving Machine Learning (PPML), as suggested by [9].

The practical implementation of DP in healthcare has been greatly facilitated by the development of open-source tools and libraries, such as Google's TensorFlow Privacy and IBM's Differential Privacy Library. These resources have democratized access to DP techniques, enabling researchers to incorporate DP into their studies with relative ease. The availability of these tools is a testament to the growing recognition of the importance of privacy in healthcare analytics and the commitment of the research community to ethical data practices. In addition to standalone DP methods, there is a burgeoning interest in hybrid privacy-preserving techniques that combine DP with other methods such as Homomorphic Encryption (HE) and Secure Multi-party Computation (MPC). These hybrid approaches can offer enhanced privacy preservation, particularly in complex healthcare scenarios involving various types of sensitive data. The work of [9] points to the potential of these hybrid techniques in advancing the field of PPML, suggesting that the integration of DP with other privacy-enhancing methods could lead to more effective and nuanced privacy solutions [9].

Despite the promise of these advanced techniques, significant challenges remain. The computational complexity of methods like HE can be a barrier to their widespread adoption in large-scale healthcare data analysis. Moreover, the efficiency of communication in FL systems is a critical issue that must be addressed to ensure that these privacy-preserving methods are scalable and practical for real-world healthcare applications [9]. The integration of DP with other Privacy-Enhancing Technologies (PETs) in the Internet of Health Things (IoHT) represents another exciting frontier in healthcare data privacy. The IoHT encompasses a vast network of connected healthcare devices that collect and transmit data, raising unique privacy and security concerns. Researchers are exploring a variety of PETs, including anonymization techniques, cryptographic methods, and blockchain technology, to bolster the privacy and security of data in the IoHT ecosystem [21].

The integration of insights from [9] into the analysis of DP in healthcare data underscores the evolving nature of this field. It highlights the importance of DP as part of a broader suite of privacy-preserving techniques and the ongoing research efforts to optimize the balance between privacy, utility, and performance. The challenges and pitfalls identified in the implementation of DP and other privacy-preserving techniques are critical areas for future research, particularly in the context of healthcare, where the implications of privacy breaches can be particularly severe. As the field continues to advance, it is clear that DP will remain a cornerstone of privacy-preserving healthcare analytics, with its role and methodologies continuing to evolve in response to emerging challenges and technological advancements.

The continuous evolution of DP in healthcare analytics is not only a response to technological advancements but also a reflection of the sector's growing emphasis on ethical data usage and the protection of patient privacy. As healthcare systems become increasingly data-driven, the need for robust privacy-preserving mechanisms becomes more pronounced. The integration of DP with other cutting-edge technologies is indicative of the dynamic nature of research in this area, where innovation is driven by the dual imperatives of safeguarding privacy and enhancing the quality of care. The exploration of future research directions is particularly pertinent in the context of privacy-aware machine learning, adversarially robust ML, distributed ML, and tiny ML. These areas represent the cutting-edge of PPML and are likely to shape the future of DP applications in healthcare. The development of privacy-aware ML algorithms, for instance, could lead to models that inherently account for privacy considerations during their training and operation, thereby embedding privacy into the very fabric of data analysis [9].

The challenges associated with implementing DP and other privacy-preserving techniques, such as the balance between data privacy and model accuracy, are not trivial. These challenges are compounded by the computational demands of advanced privacy-preserving methods and the need for efficient communication protocols in distributed learning environments. Addressing these challenges requires a concerted effort from the research community, industry stakeholders, and regulatory bodies to develop standards

and best practices that can guide the ethical use of healthcare data. Furthermore, the potential of DP to work in concert with other PETs in the IoHT is an area ripe for exploration. As healthcare devices become more interconnected, the risk of privacy breaches increases. The application of DP in this context could help to ensure that the data collected by these devices remains private, even as it is used to inform healthcare decisions and improve patient outcomes [21]. In light of these considerations, the role of DP in healthcare data analysis is multifaceted and continually expanding. It is not only a technical solution but also a commitment to the ethical stewardship of sensitive data. The integration of DP into healthcare analytics represents a proactive approach to privacy, one that anticipates and mitigates risks rather than merely responding to breaches after they occur [9].

4.2.3. Blockchain Technology: Revolutionizing Data Handling

Blockchain technology stands at the forefront of revolutionizing data handling in healthcare AI. Its decentralized nature addresses several fundamental issues associated with traditional centralized data storage systems, such as vulnerability to data breaches, manipulation, and single points of failure. The immutability feature of blockchain is particularly significant in healthcare settings. Once data, such as patient records or research findings, is recorded on a blockchain, it cannot be altered retroactively. This ensures the accuracy and reliability of medical data, which are critical in clinical decision-making and patient care. Additionally, blockchain's transparency and traceability features introduce a new level of accountability in data handling. It allows for a transparent and verifiable history of data transactions and modifications, which is particularly valuable in sensitive healthcare environments where data provenance and integrity are paramount. The technology's ability to track and record every change made to the data enhances trust and reliability, making it an indispensable tool in modern healthcare data management [9,29,32].

Blockchain technology significantly departs from traditional centralized data storage systems commonly used in healthcare. These centralized systems, typically managed by a single entity, are more vulnerable to cyberattacks and unauthorized access. Blockchain's decentralized approach, however, distributes data across a network of nodes, thereby reducing the risk of a single point of failure and enhancing resilience to attacks. Traditional systems also often struggle with data silos and interoperability challenges, whereas blockchain technology can enable seamless data exchange while upholding stringent security and privacy standards [15]. The advantages of blockchain over traditional systems are not merely theoretical but have been demonstrated through various case studies and practical applications. For instance, blockchain's application in securing electronic health records (EHRs) has resulted in a tamper-proof ledger that maintains the accuracy and integrity of patient data over time. Additionally, blockchain has been instrumental in the pharmaceutical supply chain, tracking drugs from the manufacturer to the patient, thus ensuring drug authenticity and preventing the infiltration of counterfeit medications [17].

Regarding data privacy, blockchain technology offers robust solutions through encryption and selective sharing capabilities. Sensitive patient data can be securely stored on the blockchain, with access restricted to authorized individuals only. This approach not only preserves patient confidentiality but also facilitates the necessary sharing of information for clinical treatment and research, addressing privacy concerns effectively. However, integrating blockchain with existing healthcare systems has its challenges. Issues such as technological compatibility, data standardization, and establishing a regulatory framework that recognizes the unique features of blockchain must be addressed. To overcome these obstacles, strategies such as developing interoperable platforms, establishing data standards, and collaborating with regulatory bodies are essential to ensuring compliance with healthcare regulations [17]. Looking ahead, the future of blockchain in healthcare AI is marked by several emerging trends and research directions. The development of decentralized applications (dApps) for patient engagement, the facilitation of personalized medicine through secure genomic data sharing, and the utilization of smart contracts for automating healthcare processes are areas of active exploration. Research is also focused

on improving the scalability and efficiency of blockchain networks to manage the large volumes of data generated in healthcare environments [15].

Implementing blockchain in healthcare AI also brings critical regulatory and ethical considerations to the forefront. Regulatory bodies are tasked with adapting existing frameworks to ensure blockchain applications comply with health data protection laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. Ethical considerations are equally important, with a need to ensure informed consent for data sharing, maintain patient autonomy, and address potential biases in AI algorithms that utilize blockchain-stored data. Establishing clear guidelines is essential to balance the drive for innovation with the imperative to protect patient rights [17]. Despite its potential, blockchain technology in healthcare has limitations. The scalability of blockchain networks, the energy consumption of consensus mechanisms like proof-of-work, and the challenge of integrating off-chain data are significant concerns. To address these issues, researchers and developers are exploring more energy-efficient consensus algorithms, layer-two scaling solutions, and hybrid systems that combine blockchain with other data storage methods to optimize performance and cost [15].

A detailed analysis of security threats to smart healthcare systems reveals various vulnerabilities, ranging from phishing attacks to sophisticated ransomware. Cyber attackers may target patient data for financial gain or disrupt healthcare services for political motives. Blockchain's inherent features, such as immutability and auditability, are critical in preventing unauthorized data alterations and tracing the source of attacks, thus enhancing the overall security posture of healthcare systems. Emerging technologies like AI and blockchain are increasingly crucial to bolstering security within smart healthcare systems. AI can detect anomalous behavior indicative of a security breach, while blockchain secures data transactions and ensures the integrity of health records. Together, these technologies form a robust defense against cyber threats, safeguarding the confidentiality, integrity, and availability of critical healthcare data [15]. Real-world case studies of security breaches in healthcare systems, such as the WannaCry ransomware attack in 2017, highlight the necessity for robust security measures. The attack on the UK's National Health Service, which led to the cancellation of thousands of appointments and operations, underscored the need for secure and resilient healthcare IT systems. Blockchain could have mitigated some of the risks of this incident by preventing the attack's spread through its decentralized architecture [17].

When comparing security solutions, it becomes evident that, while essential, traditional cybersecurity measures such as firewalls and antivirus software may not fully address the complex security challenges of smart healthcare systems. Blockchain technology emerges as a complementary solution, offering a tamper-evident ledger for data transactions, thus enhancing data integrity and traceability. However, blockchain should be viewed as something more than a standalone solution but as part of a comprehensive security framework that includes intrusion detection systems, advanced encryption methods, and other security technologies. This multi-layered approach is crucial for creating a robust defense against various cyber threats. The comparison underscores the importance of integrating blockchain with other advanced security solutions to establish a holistic and resilient healthcare IT infrastructure. This integrated approach strengthens the security posture of healthcare systems and ensures they are equipped to handle the evolving landscape of cyber threats.

4.2.4. Secure Multi-Party Computation (SMPC): Preserving Data Privacy

Secure Multi-party Computation (SMPC), a critical subfield of cryptography, allows for secure and private data computation across multiple parties without exposing individual data inputs. In healthcare, where data sharing is often necessary but fraught with privacy concerns, SMPC offers a solution that preserves data privacy while enabling valuable computations and analyses. For example, in genomic research or collaborative studies involving

multiple healthcare institutions, SMPC enables secure, joint computations on shared data without exposing individual patient data. Each party involved in the computation only accesses a portion of the data, ensuring the overall dataset remains confidential. This method is invaluable in scenarios like aggregating patient data from multiple healthcare providers to calculate averages or identify trends without compromising individual patient privacy. In genomic research, where sensitive data are often shared among researchers and institutions, SMPC provides a secure framework for querying genomic databases in semi-honest cloud environments. This maintains individual data privacy and enables effective and efficient search capabilities across extensive genomic datasets, paving the way for advancements in personalized medicine and genetic research [9].

Integrating Homomorphic Encryption, Differential Privacy, blockchain technology, and Secure Multi-party Computation represents more than just an advancement in data security methodologies; it heralds a new era in managing and utilizing data within AI-driven healthcare systems. These technologies, each with unique capabilities, converge to form a comprehensive security framework critical for the integrity and reliability of modern healthcare systems. Homomorphic Encryption ensures the confidentiality of sensitive data, such as genetic information and personal health histories, even during complex processing tasks, which is vital for precision medicine and personalized treatments. Meanwhile, Differential Privacy effectively maintains the anonymity of individual data points in large-scale analyses, fostering patient trust and encouraging data sharing for comprehensive medical research. This approach is crucial for advancing our understanding of diseases and improving treatment options. Blockchain technology revolutionizes data handling with its immutable and transparent ledger system, ensuring data accuracy and history in the healthcare sector. Its ability to provide a tamper-proof record of data changes bolsters trust and reliability in medical data, forming a dependable foundation for medical decisions. Complementing these technologies, Secure Multi-party Computation enables secure collaboration on sensitive data across multiple entities. This is especially important in collaborative research and cross-institutional studies, where data sharing is necessary but privacy is paramount. SMPC facilitates the aggregation and analysis of diverse data sets, enriching research while protecting individual privacy [9].

Together, these technologies form a robust and dynamic defense against AI-driven healthcare systems' myriad data security challenges. They provide the necessary tools to protect sensitive patient data while allowing the healthcare industry to leverage the full potential of AI and big data. This balance between robust data protection and functional utility in healthcare settings is not just a technical achievement but a cornerstone of pursuing advanced, personalized, and efficient healthcare services. As these technologies continue to evolve and integrate, they promise to enhance healthcare systems' security, efficiency, and efficacy worldwide, ultimately leading to better patient outcomes and a more resilient healthcare infrastructure [9].

4.3. Blockchain Technology in Healthcare AI

Blockchain technology, or distributed ledger technology (DLT), has introduced a paradigm shift in AI-driven healthcare systems, revolutionizing how patient data are stored, accessed, and secured. This dynamic blockchain ecosystem is not just a static data repository but a transformative force that brings unprecedented transparency, efficiency, and reliability to healthcare data management [18]. The intrinsic features of blockchain, such as immutability, transparency, and decentralization, have been particularly transformative in healthcare, where the accuracy and confidentiality of patient data are of utmost importance. The secure storage of patient records, the tracking of medication supply chains, and the management of consent for data sharing are all bolstered by blockchain's tamper-proof nature, which has significant implications for patient care and privacy. These capabilities are instrumental in reducing errors, preventing fraud, and enhancing the trustworthiness of digital healthcare systems [33]. However, integrating blockchain technology in healthcare AI presents complex interactions with data protection laws such as the Eu-

European Union's General Data Protection Regulation (GDPR). GDPR imposes stringent requirements on personal data processing, focusing on principles such as consent, the right to access, rectification, and the right to be forgotten. The immutable nature of blockchain creates a unique set of challenges when juxtaposed with GDPR's emphasis on data subjects' rights, necessitating a careful analysis of how blockchain's architectural features and operational mechanisms align with or diverge from GDPR principles [32].

Blockchain is not a monolithic technology but a class of technology with various forms of distributed databases, each having distinct technical and governance arrangements. This diversity means that blockchain compatibility with GDPR cannot be generalized; it must be evaluated on a case-by-case basis, considering each blockchain use case's specific technical design and governance setup. This nuanced understanding is vital in healthcare AI, where patient data security and privacy are critical. While blockchain's core features offer significant advantages for managing healthcare data, their compatibility with GDPR principles needs careful examination. For instance, GDPR emphasizes the rights of data subjects, including the right to access, rectification, and erasure ('right to be forgotten'). However, the blockchain's immutable nature poses challenges to these rights, as data modification or removal is difficult once added to the blockchain, conflicting with GDPR's requirements. Private and permissioned blockchains might be more readily designed to comply with GDPR than public and permissionless networks in healthcare AI, where data sensitivity is high. In a permissioned blockchain, participants are known and can establish contractual relationships, which facilitates compliance with GDPR's requirements for data processing and protection. Several considerations must be considered to align blockchain applications in healthcare AI with GDPR. Data Protection by Design is a principle that should be incorporated into the blockchain's architecture from the outset, ensuring that data protection is an integral part of the system. Selective Data Recording can be explored to record only essential data on the blockchain, aligning with the GDPR's data minimization principle. Consent management must be robust, especially for sensitive health data. Interoperability with existing systems is crucial to ensuring blockchain solutions can interact seamlessly with existing healthcare data systems, which might be subject to different data protection regulations. Lastly, innovative solutions for data erasure, such as advanced encryption or off-chain storage, must be investigated to address the challenges posed by blockchain's immutability to the GDPR's right to erasure [32].

The integration of blockchain and AI in healthcare has the potential to significantly improve service efficiency, reduce costs, and democratize access to medical services. Blockchain's role in preserving and exchanging patient data is particularly noteworthy for its potential to enhance data efficiency and security. The decentralized and immutable ledger that blockchain provides ensures that no single entity controls the entire dataset, enhancing security by reducing the risk of data tampering and unauthorized access. This is fundamental in healthcare, where the precision and unchangeability of medical records are critical, ensuring that patient data remain accurate and unaltered over time. Blockchain's ability to maintain a transparent and traceable record of transactions is crucial in the pharmaceutical industry for tracking medication supply chains and effectively combating counterfeit drugs. This transparency helps identify sources of falsification, thus safeguarding patient safety and ensuring the authenticity of medicines. Moreover, the confidentiality of patient records is enhanced by blockchain technology, which provides a secure way to store and manage patient records on its decentralized network, minimizing the risks associated with centralized databases. The distributed ledger architecture of blockchain implies that data are not stored in a single location but across multiple nodes, each maintaining a copy of the ledger. This contributes to the resilience and security of the system, making it significantly more difficult for attackers to compromise the integrity of the data. By enabling better control and management of health records, blockchain technology translates to more efficient patient care, as providers have secure and immediate access to up-to-date patient records. This efficiency saves time and reduces the chances of medical errors, leading to improved patient outcomes [33,34].

In resource optimization for therapies and medications, blockchain's secure storage of extensive medical data facilitates researchers in computing estimates for various treatments and remedies more effectively. This leads to more efficient and potentially more effective healthcare solutions. The requirement for a common consensus to modify records on a blockchain enhances the security of the data, ensuring that any data modification is transparent and agreed upon by all network participants. The accessibility and accountability provided by blockchain architecture are crucial in healthcare, where stakeholders from various sectors may need to interact with patient data. Blockchain technology represents a significant advancement in managing patient data, offering a robust framework for enhancing the security, efficiency, and reliability of healthcare data management [34]. The authors of [18] further elaborate on the fundamental characteristics of blockchain, describing it as a distributed database that uses state machine replication with atomic changes, referred to as transactions. These transactions are grouped into blocks and linked via hash links, ensuring integrity and tamper resistance. This decentralized structure is fundamental to blockchain's application in healthcare, ensuring secure and stable monitoring of healthcare records.

Blockchain's impact on electronic health records (EHRs) is significant, facilitating more accessible communication and control and aiding in better and faster decision-making in healthcare. The decentralized nature of blockchain allows for the maintenance of EHRs across various organizations, solving issues like data fragmentation and access limitations patients face when their life circumstances change. Specific blockchain-based systems like 'MedRec' and 'MeD Share' have been developed to operate on a decentralized basis for maintaining data and claims, providing patients with complete and permanent access to their clinical documents, and focusing on data protection and privacy across different healthcare stakeholders. Smart contracts deployed in healthcare maintain transparency across multiple stages of medical studies. They are scripts processed on a blockchain, ensuring the authenticity and confidentiality of patient data. For instance, blockchain-based telemonitoring healthcare systems can detect and manage cancerous cells, utilizing smart contracts to ensure data integrity. Blockchain technology also ensures the provenance of medical commodities. In the pharmaceutical industry, it allows for tracking items from manufacturing through each stage of the supply chain, ensuring that the final product delivered to the consumer is genuine and has not been tampered with. This traceability is crucial in preventing the distribution of counterfeit drugs, which can have profound implications for patient health and safety. By providing a transparent and immutable supply chain record, blockchain technology helps establish trust among consumers, healthcare providers, and regulatory bodies. Moreover, blockchain can facilitate the secure sharing of medical data for research while preserving patient anonymity. This is particularly important for advancing medical research and developing new treatments, as large datasets are often required. By using blockchain, researchers can access a wealth of de-identified patient data without compromising individual privacy, thus accelerating the pace of medical innovation [18,34].

The potential of blockchain in healthcare extends to insurance and billing, where it can streamline processes and reduce fraud. Smart contracts can automatically execute claim processing, reducing the need for intermediaries and minimizing the risk of fraudulent claims. This leads to cost savings for healthcare providers and insurers and improves the overall patient experience by expediting the reimbursement process. Despite these advantages, implementing blockchain in healthcare AI systems must be approached cautiously, considering the regulatory and ethical implications. The challenges posed by GDPR and other data protection laws must be addressed through innovative solutions that reconcile blockchain's immutability with the need for data rectification and erasure. Furthermore, the technical complexity of blockchain may present barriers to adoption, requiring significant investment in infrastructure and education for healthcare professionals and patients alike. Blockchain technology is promising to revolutionize healthcare AI systems by enhancing data security, transparency, and efficiency. Its applications range from secure patient record management to supply chain integrity and research data sharing. However, the successful

integration of blockchain into healthcare will depend on careful consideration of legal and ethical issues and a commitment to overcoming technical and operational challenges. As the technology matures and solutions to these challenges are developed, blockchain is poised to play a pivotal role in the future of healthcare, potentially leading to more personalized, efficient, and secure medical services for patients worldwide [18,34].

4.3.1. Fundamental Nature of Blockchain

Fundamentally, a blockchain is a shared and synchronized digital database maintained through a consensus algorithm across multiple nodes. Each node, essentially a computer, stores a complete version of this database and can independently update it. This decentralized structure of blockchains, with data stored and processed across various nodes, not only enhances resilience through replication but also ensures that multiple custodians are involved in the upkeep of the ledger. This decentralized approach is critical in healthcare AI, where the integrity and availability of data can directly impact patient outcomes. By their very nature, blockchains are append-only ledgers, meaning that while data can be easily added, its removal is possible only under exceptional circumstances. Blockchain is not a singular technology but represents a broad class of distributed databases, varying in technical and governance arrangements. This variety means that blockchain compatibility with regulations like the GDPR must be assessed case-by-case, considering each blockchain application's specific design and governance. In healthcare, this implies carefully evaluating each blockchain application's design to ensure compliance with healthcare regulations and data protection laws [32].

Blockchain technology goes beyond mere data storage; it is also a programmable platform, enabling applications such as smart contracts. These smart contracts can automate processes in healthcare AI, from patient consent management to supply chain tracking. The blockchain ecosystem is multilayered, relying on the Internet and TCP/IP for its operation and serving as an infrastructure for data management. It can store data directly or as a linkage system, functioning as a shared accounting system across multiple actors. This ability to standardize and link data across a decentralized network is particularly beneficial in healthcare, where multiple stakeholders, including healthcare providers, patients, and insurers, must coordinate and share information efficiently and securely. While essentially digital, the data stored on blockchains can represent a wide array of assets or rights. For instance, blockchain-based assets can represent real-world objects or entitlements, offering a new way to manage and track assets and rights in the digital world. This aspect is significant in healthcare for managing digital assets like patient records or intellectual property in medical research [32].

Blockchains are categorized into public, permissionless, private, and permissioned networks. In public, permissionless blockchains, anyone can participate without needing permission. These networks are characterized by transparency, as their complete ledger can be accessed by anyone, enhancing public auditability but reducing privacy. In contrast, private, permissioned blockchains run on private networks, where participants require permission from a network administrator to join. These networks are often designed for specific purposes and offer greater control over who has access to the network and its data. This control is crucial in healthcare, where patient data privacy and regulatory compliance are paramount. While public blockchains offer pseudonymity, private blockchains usually involve known identities, at least to the network gatekeepers. Blockchain technology in healthcare AI represents a complex, multifaceted system that offers significant data integrity, security, and efficiency benefits. Its diverse nature requires carefully considering each application to ensure it aligns with healthcare and data protection standards. As healthcare continues to embrace digital transformation, blockchain is a pivotal technology, promising enhanced security, transparency, and efficiency in handling sensitive healthcare data [32].

4.3.2. Blockchain and GDPR: Analyzing the Tensions and Synergies

The intricate relationship between blockchain technologies and the General Data Protection Regulation (GDPR) is fraught with complexities and tensions. These arise from the fundamental disparities in their core principles and how they operate. Blockchain, known for its revolutionary approach to data management, clashes with GDPR's established data protection framework in several critical ways. At the heart of the conflict is the issue of decentralization versus centralized data controllership. The GDPR is built on the premise that personal data should have an identifiable controller, an entity responsible for safeguarding the data subject's rights as stipulated by the regulation. This centralized approach ensures accountability and a point of contact for individuals to exercise their rights. In stark contrast, blockchain technology is predicated on the principle of decentralization. It distributes the responsibilities of data controllership across a network of participants, making it difficult to pinpoint a single responsible party. This diffusion of responsibility challenges the notion of controllership as defined by the GDPR, leading to legal ambiguities and difficulties enforcing data protection rights [32].

Another point of contention is the clash between blockchain data immutability and GDPR's data modification and erasure provisions. The GDPR enshrines the rights of individuals to have their data corrected or deleted under certain conditions, as outlined in Articles 16 and 17. These rights are essential for maintaining data accuracy and respecting individuals' wishes to 'be forgotten'. However, the blockchain's architecture is intentionally resistant to changes; once data are added, it is meant to be permanent. This immutability is a cornerstone of blockchain's security and trustworthiness but directly opposes the GDPR's requirements for data modification and erasure. The result is a complex puzzle of reconciling blockchain's unchangeable ledger with the GDPR's flexible approach to personal data management. Furthermore, blockchain's design raises questions about GDPR principles such as data minimization and purpose limitation. The technology's append-only ledger, which grows continuously and replicates data across numerous nodes, seems at odds with the GDPR's mandate to limit personal data collection and usage to what is strictly necessary for specific purposes. The interpretation of the 'purpose' of data processing in a blockchain context—whether it refers only to the initial transaction or extends to ongoing data processing—is yet to be clearly defined [32].

Despite these challenges, blockchain technology promises to enhance certain aspects of GDPR compliance. For instance, blockchain can serve as a robust tool for data governance, offering new ways to manage and distribute data without relying on a central authority. This decentralized approach can increase transparency in data transactions and potentially streamline the process of data sharing. By utilizing smart contracts, blockchain can automate these transactions, thereby reducing costs and altering the dynamics of data exchange. Moreover, blockchain can potentially empower individuals with greater control over their data, which aligns with the GDPR's objectives. For example, blockchain can facilitate the exercise of rights such as access to personal data (Article 15 GDPR) and data portability (Article 20 GDPR). These provisions give individuals a say in how their data are used and quickly transfer it from one service provider to another. By leveraging blockchain, data subjects could monitor how their data are being used, ensuring adherence to GDPR principles like purpose limitation and quickly identifying any breaches or misuse of their data [32].

Blockchain's attributes could also be advantageous for developing Artificial Intelligence (AI) and creating data marketplaces within the European Union. By providing a secure and transparent environment for data sharing, blockchain can facilitate the pooling of data necessary for AI research while still upholding GDPR standards. This could be particularly beneficial for institutions that require access to large datasets to train AI algorithms but must do so in a manner that respects privacy and data protection laws. Integrating blockchain technology with GDPR requirements presents a complex landscape of challenges and opportunities. The decentralized nature and data immutability of blockchain are at odds with GDPR's centralized controllership model and its flexibility

regarding data management. However, blockchain also offers potential benefits supporting GDPR's goals, such as improved data governance and enhanced control for data subjects. Navigating this terrain requires a careful and context-specific approach, considering each blockchain implementation's unique technical and operational characteristics. The goal is to find a harmonious balance that harnesses the strengths of blockchain while ensuring full compliance with the stringent data protection standards set forth by the GDPR [32].

4.4. Advanced Data Validation Algorithms

The role of advanced data validation algorithms is indispensable in AI healthcare, particularly in areas like precision medicine and genomics. These sophisticated algorithms are the cornerstone for maintaining data integrity, playing a crucial role in the continuous monitoring and verification of healthcare data's accuracy and consistency. Such vigilance is vital for AI systems to make timely and precise decisions. By rigorously comparing incoming data with established medical standards and protocols, these algorithms guarantee the medical accuracy and relevance of the data utilized in AI analyses. Their flexibility is critical, allowing for updates in tandem with the ever-evolving landscape of medical knowledge and practices. This dynamic validation process ensures that AI systems remain accurate and relevant in the fast-paced healthcare field. It serves as a safeguard, keeping the input data for AI healthcare systems precise but also up-to-date and pertinent. As illustrated in Table 3, these algorithms act as crucial gatekeepers, ensuring that the data inputted into healthcare AI systems is accurate, current, and relevant. This pivotal role significantly diminishes the risk of misdiagnoses or inappropriate treatment recommendations arising from outdated or erroneous data, thereby reinforcing the trust and effectiveness of AI in healthcare decisions [9,29].

4.5. Collective Contribution to Reliable AI in Healthcare

Integrating blockchain technology with advanced data validation algorithms marks a significant advancement in ensuring data integrity within healthcare AI. This combination comprehensively addresses the multifaceted challenges of data management and security in healthcare settings. Blockchain technology provides a groundbreaking platform for secure and immutable data storage, ensuring that patient records and clinical trial information are protected from tampering and unauthorized access. The decentralized and transparent nature of blockchain ensures that data modifications are recorded and traceable, enhancing trust and reliability in the data used by AI systems. Concurrently, advanced data validation algorithms act as a second defense layer, continuously ensuring the accuracy and consistency of healthcare data. These algorithms are crucial in identifying and correcting any anomalies or inaccuracies in patient data before AI systems use them. The collective impact of integrating these technologies is substantial. These technologies foster trust among healthcare professionals and patients by securing data integrity and maintaining quality. They pave the way for AI to augment healthcare delivery with the utmost reliability and trustworthiness, addressing national efficiency, patient safety, and treatment outcomes. This synergistic approach represents a commitment to harnessing the power of AI in healthcare in a manner that respects the integrity of data and, by extension, the integrity of healthcare services and patient care [29].

The combined impact of technologies like blockchain and advanced data validation algorithms profoundly ensures reliable AI in healthcare. These technologies provide a robust data integrity, security, and privacy framework. The evolution of privacy-preserving techniques, including PPML, HE, and SMPC, highlights the ongoing efforts to enhance data security in healthcare AI. These advancements point towards future challenges and potential developments in balancing privacy with data utility and managing communication costs in systems like Federated Learning. Integrating various privacy-preserving strategies through hybrid techniques offers promising solutions to complex privacy concerns in AI healthcare systems [9].

Table 3. Comprehensive summary of advanced data validation algorithms: benefits and challenges.

Feature	Benefits	Challenges	Additional Considerations	Integration with Existing Systems	Resource and Cost Implications
Real-time Validation	Immediate accuracy and consistency checks	Constant monitoring and updating needed	Balancing accuracy with system load	Seamless integration required	May increase operational costs
Adaptability to Evolving Data	Keeps pace with new medical data and practices	Complexity in maintenance and updates	Aligning with medical advancements	Requires flexible system design	Resource-intensive for ongoing updates
Anomaly Detection	Identifies and corrects data errors	Resource-intensive for computing resources	Prioritization in data areas	Must align with AI objectives	Involves investment in advanced hardware
Scalability	Efficient handling of large data volumes	Technical hurdles in scaling algorithms	Developing scalable solutions	Compatibility with large datasets	High cost for scaling infrastructure
Integration with AI Systems	Enhances the effectiveness of AI healthcare applications	Alignment of algorithms with AI objectives needed	Ensuring compatibility and effectiveness	Smooth integration is essential	Requires dedicated resources for setup
Data Accessibility	Centralized control	Distributed access enhances availability	Ensuring equitable access	Improves data availability	Requires effective data distribution
Ethical Considerations	Ensures adherence to moral and ethical guidelines	Balancing innovation with ethical constraints	Inclusion of diverse stakeholder perspectives	Ethical Considerations	Ensures adherence to moral and ethical guidelines
Privacy Protection	Safeguards patient data against breaches	Implementation of robust security measures	Compliance with data protection laws and standards	Privacy Protection	Safeguards patient data against breaches
Transparency and Accountability	Enhances trust and reliability in AI applications	Challenges in explaining AI decisions to non-experts	Regular audits, clear documentation, and error reporting	Transparency and Accountability	Enhances trust and reliability in AI applications

4.5.1. Hybrid Privacy-Preserving Techniques in Healthcare AI

In the realm of healthcare AI, the adoption of hybrid privacy-preserving techniques signifies a significant leap in safeguarding data privacy and integrity. These techniques combine various privacy strategies to excel in complex situations in healthcare settings. By integrating a range of methods, they overcome the limitations of single-strategy approaches, resulting in more robust and private models. A prime example of such a hybrid approach is the fusion of Homomorphic Encryption (HE) and Differential Privacy (DP). HE allows for processing encrypted data without decryption, thus maintaining privacy. DP introduces an anonymity layer in tandem, making this combination highly effective in scenarios that demand encryption and data anonymity. Further enhancement in data security is achieved through integrating blockchain technology with either HE or DP. When paired with the privacy capabilities of HE or DP, the immutable ledger of blockchain significantly improves the overall security and confidentiality of data. This is particularly beneficial for securely logging data access and processing records, ensuring the data remain protected and private. Additionally, the integration of Secure Multi-party Computation (SMPC) with blockchain technology harnesses the distributed computation power of SMPC along with the secure, transparent ledger of the blockchain. This combination promotes collaborative data analysis and processing across various entities while safeguarding the privacy and security of each participant's data [9]. These advanced hybrid techniques demonstrate the innovative strides

in healthcare AI to address complex privacy concerns, showcasing a blend of multiple privacy-preserving strategies to handle the intricacies of this field effectively.

4.5.2. Advancing Healthcare AI with Synthetic Data Generation: Challenges and Opportunities

The field of healthcare AI has seen significant advancements with the introduction of synthetic data generation, a concept highlighted by the role of Synthea, an open-source tool designed for creating synthetic medical data. Synthea, tailored explicitly for research purposes, generates ‘realistic but not real medical data’, mimicking accurate patient data in structure and composition without corresponding to individual patient information [23]. This innovative approach is vital for maintaining patient privacy and the integrity of AI models, enabling the development and testing of healthcare AI applications without the risk of exposing sensitive patient information.

The application of synthetic data in research and development is particularly noteworthy. By providing rich datasets, Synthea and similar tools allow for developing and refining AI models, conducting analyses, and exploring new healthcare technologies while safeguarding patient privacy. Synthetic data generation is pivotal in ensuring the privacy and security of healthcare data, especially in AI applications, as it allows for the use of comprehensive and realistic datasets without compromising patient confidentiality. This supports the safe and ethical development of AI technologies in healthcare [23].

The complexities and challenges of generating synthetic electronic health records are explored in depth, focusing on creating large databases encompassing linear and nonlinear associations among medical elements and random associations. This process is essential to accurately replicating the intricate patterns in real-world health data. A primary constraint in this endeavor is the size of the databases utilized. Smaller databases may only partially capture the extensive statistical characteristics of the original data, which can impact the realism and utility of the synthetic data. Additionally, preserving the interactions and correlations in the original data introduces another layer of complexity, necessitating the comprehensive capture of high-order relationships within the data. The field also faces the challenge of a lack of established metrics to assess the realism of the generated data, particularly in medical imaging. This makes it difficult to evaluate how closely the synthetic data mirrors the original and its usefulness for research purposes. Clinician validation of synthetic data, especially in medical imaging, is pivotal to ensuring its high quality and reliability for research and development purposes [12].

Synthetic data, replicating the statistical characteristics and correlations of original data, overcomes common data-sharing obstacles, allowing for secure access and sharing across institutions. This method protects patient privacy while preserving data utility. Synthetic data’s potential for building large datasets is highlighted, suggesting that scientific studies could publish corresponding synthetic data in international journals instead of original datasets. While there is only a slight decrease in accuracy for models trained with synthetic data compared to those trained with accurate data, challenges in synthetic data generation remain, especially in medical imaging. These include validating the realism of generated data, capturing high-order and complex relationships, and the lack of metrics for evaluating the realism of generated data. Additionally, assessing human perception and judgment of generated images remains a limitation. In conclusion, synthetic data generation is crucial to maintaining privacy and security in healthcare AI applications, enabling the creation of extensive datasets for research and development while protecting patient privacy and AI model integrity. However, it faces challenges related to data realism and validation [12].

5. Establishing Ethical and Legal Frameworks in AI-Driven Healthcare: Navigating Technological Advancements and Regulatory Challenges

5.1. Developing Ethical and Regulatory Frameworks in AI-Driven Healthcare

Developing adaptable and responsive legal and regulatory frameworks is critical in the rapidly evolving landscape of AI-driven healthcare. These frameworks are essential for

harnessing AI's potential in healthcare and ensuring its ethical application, safeguarding patient rights, and maintaining data privacy. These policies should enhance transparency and facilitate informed patient consent, aligning with the core legal and ethical values intrinsic to healthcare. The urgency for comprehensive global legal and regulatory frameworks to keep pace with rapid advancements in AI technologies is underscored. Such robust and adaptable frameworks must address unique challenges, including decision-making autonomy, algorithmic discrimination, data privacy, and security [1,35]. Establishing a data governance panel consisting of diverse stakeholders like patient representatives, clinical experts, ethicists, and AI specialists is crucial to ensuring ethical AI implementation in healthcare. This panel would ensure that AI systems are developed with a focus on patient-centric care and that training datasets represent diverse patient populations, preventing biases that could lead to skewed healthcare outcomes. This approach also addresses the need for explainability in AI systems and their potential impacts on human dignity and integrity. It emphasizes a balanced approach, integrating rapid technological advancements with ethical considerations [2,36–38].

Challenges and Considerations in the Commercialization of AI in Healthcare

Building on this foundation, integrating AI in healthcare, particularly in fields like radiology, organ allocation, and surgery, is bringing transformative changes. These advancements, while beneficial, also present significant challenges, such as managing AI development to maximize benefits and minimize risks, including the biases and errors inherent in AI technologies. AI algorithms' 'black box' nature, which obscures their decision-making processes, raises concerns about reliability and potential errors. Concurrently, the commercialization of AI technologies, transitioning from academic research to private entity control, introduces new privacy and security concerns regarding patient health information. This shift necessitates reevaluating how patient data are accessed, used, and protected, taking into account the commercial interests of these entities [2,38].

The involvement of major technology corporations like Google, Microsoft, and Apple in healthcare AI, requiring access to vast amounts of patient health data, further amplifies these privacy issues. This development, particularly in public-private partnerships, prompts the need for stringent measures to safeguard patient data and ensure ethical usage. The deployment of AI in healthcare, marked by challenges like potential errors, biases, and opaque learning algorithms, underscores the importance of tailored regulatory systems. These systems should be designed to address AI's unique features in healthcare, ensuring transparency and accountability in AI-based decision-making processes [37,38].

Furthermore, private corporations' control of patient health information in AI applications poses significant privacy risks, with instances of inadequate privacy protection calling for stringent regulation and oversight. This regulation should emphasize patient agency, consent, and robust data anonymization and protection strategies. The evolving nature of AI and algorithms introduces risks to the security of health information, even when anonymized. Studies showing the feasibility of reidentifying anonymized data highlight the need for advanced data protection and anonymization methods. Implementing commercial healthcare AI raises several legal and ethical issues, including the necessity of patient consent and data protection. The proposal to use synthetic patient data for machine learning without compromising real patient data privacy emerges as a potential solution to these concerns. As AI continues to promise significant improvements in health outcomes, its commercial implementation faces privacy challenges. Regulation must evolve to protect patient privacy, ensure informed consent, and develop innovative data protection methods, balancing AI benefits with ethical considerations and patient rights [1,37].

5.2. Regulatory Challenges in AI Healthcare: Adapting to AI's Evolving Nature

The distinctive nature of AI systems, especially their ability to adapt and learn over time, presents a complex landscape of regulatory challenges. This dynamic aspect of AI necessitates a regulatory framework that is flexible and responsive to ongoing technological

advancements. In healthcare, where AI systems are particularly transformative, continuous monitoring and evaluation are paramount to ensuring these systems remain safe, effective, and ethically aligned over time. Such a paradigm shift in regulatory policy is crucial for adapting to the rapid technological advancements in AI. A collaborative approach involving various stakeholders is emphasized for effective AI regulation, particularly in high-risk applications like healthcare. A risk-based approach is advocated, tailoring the level of regulatory scrutiny to the potential risks and impacts of specific AI applications. This strategy aligns well with the unique demands of AI in healthcare. Delving deeper into the evolving nature of AI, we see that these systems, particularly in healthcare, are not static entities. Their capacity to learn and adapt over time means their capabilities can significantly change post-deployment. This evolving nature challenges traditional regulatory frameworks typically designed for static technologies, thus necessitating a more innovative and adaptive regulatory approach [2].

5.2.1. Navigating Regulatory Challenges in the Dynamic AI Healthcare Landscape

Addressing concrete examples of regulatory challenges further elucidates this complex landscape. Traditional regulatory standards for assessing the safety and efficacy of medical software may be ill-suited to the dynamic nature of AI. AI algorithms, especially those based on machine learning, can undergo changes and improvements over time, potentially altering their performance and safety profile post-approval. Additionally, concerns regarding liability and accountability arise when AI systems malfunction or cause harm in a healthcare setting. Current legal frameworks may not be equipped to address these new challenges, such as determining liability when an AI system's decision results in a medical error. Moreover, the heavy reliance of AI systems on large datasets, often containing sensitive patient information, poses significant challenges to data privacy and security, especially as AI systems require continuous access to new data to learn and improve [2].

5.2.2. Evolving Regulatory Frameworks for AI in Healthcare: Safety, Ethics, and Accountability

Adapting regulatory frameworks is essential for AI's safe and ethical integration in healthcare. Continuous monitoring and updating of AI systems post-deployment are critical to ensuring their ongoing safety and efficacy. This process should include regular assessments of AI systems' regulatory status based on real-world performance and impact. Transparent reporting and accountability frameworks are necessary for addressing regulatory challenges, which require clear documentation of AI decision-making processes, data sources, and methodologies. A collaborative approach that includes regulatory bodies, healthcare providers, AI developers, and patients is vital for developing flexible and responsive regulatory frameworks that can keep pace with technological advancements. A risk-based approach to regulation is also crucial, tailoring the scrutiny and regulatory requirements to the potential risks and impacts of specific AI applications, particularly those involved in critical healthcare decisions [2].

Ethical considerations, such as fairness, non-discrimination, and respect for patient autonomy, must be woven into the regulatory frameworks governing AI in healthcare. This includes proactively addressing potential biases in AI models that could lead to disparities in healthcare outcomes. The dynamic nature of AI technologies and the regulatory frameworks that govern them underscores the need for regulatory systems to evolve to match AI advancements. This evolution is significant in assessing AI's safety and efficacy, where traditional methods for evaluating medical software may not suffice. Furthermore, the liability and accountability associated with AI-driven decisions in healthcare add complexity to the regulatory landscape. Data privacy and security concerns are amplified by AI's reliance on large datasets, making it imperative that regulatory frameworks are robust enough to protect patient information while fostering innovation. Adapting the regulatory frameworks for AI in healthcare is a multifaceted endeavor that involves continuous monitoring, collaborative and risk-based approaches, transparency, and ethical considerations,

ensuring that AI applications in healthcare remain safe, effective, and aligned with societal values [2,27].

5.2.3. Regulatory Adaptation for Advanced AI Models in Healthcare

The emergence of advanced AI models like LLMs, including GPT-4, poses new challenges for regulatory bodies like the FDA, which have previously overseen AI-based medical technologies. These models' scale, capabilities, and potential impact necessitate reevaluating existing regulatory frameworks. The real-time adaptation of LLMs and the adaptive and autodidactic functions of deep learning algorithms call for regulatory frameworks capable of addressing these systems' adaptability and self-teaching nature. To address these challenges, there is a need to create new regulatory categories specifically for LLMs, distinct from existing AI-based medical technologies. Continuous monitoring and validation of these systems are crucial to ensuring their accuracy and validation across different populations. Ensuring transparency and interpretability in AI decision-making processes is also essential, albeit challenging, due to the complex nature of AI algorithms. Lastly, the regulation of AI in healthcare must consider ethical aspects, including fairness, non-discrimination, and respect for patient autonomy, to prevent potential biases in AI models that could lead to healthcare disparities. Adapting regulatory frameworks for AI in healthcare is imperative to manage the unique challenges posed by evolving AI technologies effectively. This adaptation requires a multifaceted approach, encompassing continuous monitoring, creating new regulatory categories for advanced models like LLMs, focusing on transparency, ethics, and data privacy, and integrating ethical considerations into the regulatory process [27].

5.3. Blockchain and GDPR: An In-Depth Analysis

Integrating blockchain technology with the General Data Protection Regulation (GDPR) presents a multifaceted and intricate challenge. As highlighted in the study [29], the diverse nature of blockchain technologies makes a broad assessment of their compatibility with EU data protection law impractical. This diversity is particularly evident in data modification and erasure approaches, which conflict with key GDPR provisions, notably Articles 16 and 17. These articles assume the possibility of modifying or erasing data to comply with legal requirements, a feature at odds with the typical functionality of blockchain systems. There is a notable distinction between private and permissioned blockchains, which generally align more closely with GDPR, and public and permissionless ones, which often do not. It is crucial to individually assess the compatibility of each blockchain type with the GDPR [25,32].

5.3.1. Reconciling Blockchain Technology with GDPR Compliance Challenges

The GDPR assumes the presence of identifiable data controllers for each personal data point, a notion challenged by blockchain's decentralization, which replaces a unitary actor with multiple players. This decentralization complicates the allocation of responsibility and accountability, particularly in light of the uncertain definitions of (joint) controllership under GDPR. This lack of clarity is further compounded by recent case law developments that have yet to interpret these concepts definitively. Moreover, the GDPR's provisions, particularly Articles 16 and 17, assume that data can be modified or erased as needed to comply with legal requirements. However, blockchain technologies are typically designed to make data modifications purposefully onerous, ensuring data integrity and network trust. This design principle creates a significant challenge in aligning with the GDPR's requirements for data amendment and erasure, a topic widely discussed in recent years [32].

In addition, the principles of data minimization and purpose limitation, central to GDPR, pose challenges when applied to blockchain technologies. Blockchains, being append-only databases that continuously grow with each new data entry, inherently conflict with the principle of data minimization. The application of the purpose limitation principle is also unclear in the blockchain context, particularly regarding whether it includes

only the initial transaction or the continued processing of personal data for other purposes, such as consensus or storage on the chain. These aspects underscore the complexities and challenges of reconciling the operational principles of blockchain technologies with GDPR requirements [32]. The intricate nature of these challenges, especially concerning the allocation of responsibility, data modification, data minimization, and purpose limitation, illustrates the need for detailed and nuanced approaches to ensure compliance, as comprehensively compared in Table 4.

Table 4. In-depth comparison of traditional data storage and blockchain in GDPR compliance.

Aspect	Traditional Data Storage	Blockchain Technology	Considerations and Challenges	Impact on User Privacy	Technological Adaptability
Data Modification	Supports GDPR alignment	Challenges in modification	Balancing blockchain with GDPR	Maintains user control over data	Requires innovative solutions
Data Erasure	Complies with ‘right to be forgotten’	Difficulties in data removal	Exploring technical solutions	Protects individual privacy	Needs adaptable data management
Data Security	Vulnerable to centralized attacks	Enhanced via decentralization	Developing robust cybersecurity	Increases data protection	Enhances security with decentralization
Data Transparency	Varies in transparency	High transparency due to ledger system	Balancing transparency with privacy	Ensures data traceability	Can be technically complex
Accountability	Clear responsibilities under GDPR	Complexities in defining roles	Clarifying legalities in blockchain	Enhances legal compliance	May require regulatory adjustments
Data Accessibility	Centralized control	Distributed access enhances availability	Ensuring equitable access	Improves data availability	Requires effective data distribution
Data Controllers and Joint Controllers	Clearly defined in GDPR	Complexities in private/public blockchains	Defining roles under GDPR in blockchain context	Enhances clarity in data management	Data Controllers and Joint Controllers
Data Minimization and Purpose Limitation	Required by GDPR	Challenged by blockchain’s nature	Aligning blockchain’s append-only nature with GDPR	Affects scope of data storage	Data Minimization and Purpose Limitation
Technical Solutions for GDPR Compliance	Traditional methods available	Development of blockchain-centric solutions	Exploring zero-knowledge proofs, chameleon hashes, etc.	Potential for improved compliance	Technical Solutions for GDPR Compliance
Legal Grounds for Processing Personal Data	Defined under GDPR	Varied interpretations in blockchain	Assessing legal basis for data processing in blockchain	Determines the extent of user control	Legal Grounds for Processing Personal Data
Data Subject Rights	Clearly defined rights and mechanisms	Technical and governance challenges	Application of rights like access, rectification, erasure	Direct impact on user autonomy	Data Subject Rights
Data Protection by Design and Default	GDPR compliance essential	Blockchain’s potential alignment	Leveraging blockchain for GDPR’s design and default requirements	Enhances proactive data protection	Data Protection by Design and Default

5.3.2. Addressing Legal Uncertainties in Blockchain and GDPR Compliance

Regulatory guidance is needed due to the legal uncertainties surrounding applying European data protection law to blockchain technologies. This uncertainty largely stems from blockchain's inherent technical structure and governance arrangements, which often present challenges that are at odds with GDPR requirements. Critical areas of ambiguity include the interpretation of concepts like anonymization and the definition of (joint) data controllers, leading to a lack of consensus among supervisory authorities in the European Union. Furthermore, the study highlights that core principles of GDPR, such as data minimization and purpose limitation, prove challenging when applied to the unique characteristics of blockchain and other modern data economy expressions like big data analytics. To enhance legal certainty, the study suggests the need for regulatory guidance on applying these concepts specifically to blockchain technologies. This could involve coordinated efforts by supervisory authorities and the European Data Protection Board to draft specific guidelines on GDPR application to blockchain. Additionally, updating certain opinions of the Article 29 Working Party, particularly those concerning anonymization techniques, could further clarify and solidify legal guidelines for the blockchain industry and beyond [32].

5.3.3. Facilitating GDPR Compliance in Blockchain through Codes of Conduct and Certification

Alongside regulatory guidance, supporting the development of codes of conduct and certification mechanisms is crucial. The GDPR is designed as a technologically neutral framework that can be applied to any technology, including blockchain. This principle-based regulation comprises overarching principles that must be tailored to specific personal data processing operations. The study underscores the importance of certification mechanisms and codes of conduct as GDPR tools to facilitate the application of these principles in specific contexts, especially where personal data are processed. This co-regulatory approach, where regulators and the private sector collaborate to uphold European data protection law principles, is exemplified in its application in fields such as cloud computing. These tools represent a critical strategy for ensuring GDPR compliance in varied blockchain applications, bridging the regulation's high-level principles and the practical realities of technology implementation [32].

5.3.4. Developing a Global Ethical and Regulatory Framework for AI in Healthcare

In the realm of AI healthcare applications, the intersection of ethical and regulatory concerns is of paramount importance. The urgency of developing a comprehensive global legal and regulatory framework tailored explicitly for AI in healthcare is underscored by the author of [1]. Such a framework must be adaptable to the rapid advancements in AI technology and ensure that these technologies are utilized ethically and securely within healthcare settings. This adaptability is critical due to the unique challenges posed by AI that traditional regulatory measures may not fully address. The framework should be robust and adaptable, capable of evolving alongside technological advancements while safeguarding ethical norms to ensure the beneficial application of AI in healthcare.

Furthermore, the proposal [2] for establishing a data governance panel in AI healthcare applications highlights the need to mitigate biases in AI systems. The panel, comprising diverse stakeholders including patient representatives, clinical experts, ethicists, and AI specialists, would play a vital role. Their collective responsibilities would involve reviewing and monitoring the datasets used for training AI systems, ensuring that these datasets encompass a variety of demographic groups, clinical scenarios, and health conditions to avoid biases that could result in skewed or unfair outcomes in healthcare delivery. Additionally, the panel would be responsible for the ongoing monitoring of AI systems post-deployment, continuously assessing their performance and ensuring their fairness and alignment with the evolving needs and demographics of the patient population. The collective insights from [1,36–38] emphasize the imperative balance between rapid technological advance-

ments in AI and the ethical considerations guiding their application in healthcare. This balance is essential for respecting patient privacy and agency, addressing potential biases, and upholding human dignity and integrity in patient care. A comprehensive ethical and regulatory framework is thus needed to tackle issues such as decision-making autonomy, algorithmic discrimination, data privacy, and security, considering the unique challenges posed by AI, such as the need for explainability and the potential impacts on human dignity and integrity.

5.4. Impact of Emerging Technologies on Regulations

The swift advancement of neural networks and advanced machine learning in healthcare, coupled with the rise of blockchain technology, is ushering in a new era of medical diagnostics and treatments powered by their robust data processing and analytical capabilities. However, these innovative technologies are pushing the limits of existing legal frameworks, particularly in healthcare regulation. The complexity and sophistication of neural networks in making medical predictions and decisions highlight the urgent need for more agile and responsive regulations. Similar challenges arise with integrating blockchain technology into healthcare, especially concerning the General Data Protection Regulation (GDPR). Blockchain technology underscores several regulatory tensions within the GDPR framework. Its decentralized nature contradicts the GDPR's premise of identifiable data controllers, thereby complicating the allocation of responsibilities and accountability. Moreover, the inherent difficulty of modifying or erasing blockchain data presents a direct challenge to GDPR compliance, particularly regarding data erasure interpretations. Furthermore, blockchain's append-only and ever-expanding structure conflicts with GDPR's data minimization and purpose limitation principles [32].

5.4.1. Adapting Regulatory Frameworks for AI and Blockchain in Healthcare

Regulatory frameworks must emphasize adaptability and responsiveness in light of these technological advancements. This necessitates a reevaluation and potential reformation of conventional healthcare laws and ethical guidelines, considering AI's decision-making capabilities. Additionally, integrating blockchain technology into healthcare systems demands specific regulatory guidance in line with GDPR. This guidance should clarify concepts such as anonymization and data controllership and leverage GDPR's technology-neutral design. Certification mechanisms and codes of conduct could effectively apply GDPR principles to blockchain-specific scenarios [32].

5.4.2. Evolving Healthcare Regulations to Address Emerging AI and Blockchain Technologies

The dynamic nature of neural networks, machine learning, and blockchain technologies necessitates that regulations evolve to cover new forms of data processing and medical applications comprehensively. This evolutionary approach is crucial to safeguarding patient safety, ensuring data privacy, and promoting ethical AI usage in healthcare. Moreover, it is essential to address the unique challenges of emerging technologies like blockchain, which operate under current data protection laws. These challenges include privacy concerns related to large tech corporations dominating machine learning and neural network technologies, issues surrounding generative models for patient data, and the implications of AI technologies in healthcare domains like oncology, organ allocation, and robotic surgery [1]. The regulatory lag behind technological advancements, the global legal and regulatory framework needs, data privacy concerns in public–private partnerships, and the risks of reidentification in big data usage are all critical factors that must be considered in developing future healthcare regulations.

5.5. Patient Rights and Informed Consent in AI Healthcare

The integration of Artificial Intelligence (AI) in healthcare has brought about a paradigm shift in the dynamics of patient consent, necessitating a reevaluation of traditional informed

consent models to accommodate the unique challenges posed by AI technologies. The conventional approach, where patients are informed about the risks and benefits of medical procedures or treatments, is no longer sufficient in AI-driven healthcare. Instead, a more nuanced and ongoing consent process is required to address the complexities introduced by AI systems. AI and privacy concerns are at the forefront of this shift. The increasing control of patient health information by private corporations due to public-private partnerships in AI implementation raises significant challenges in ensuring privacy and patient agency. These corporations may have competing goals that do not prioritize data protection, thus complicating the consent process. Additionally, the opaque nature of AI systems, often described as ‘black boxes’, makes it difficult for medical professionals to supervise or understand the decision-making processes of algorithms, further necessitating more robust safeguards for patient data [1,2].

5.5.1. Adapting Consent Processes to Address Reidentification Risks in AI Healthcare

The risk of reidentifying anonymized patient data using advanced AI algorithms is a pressing concern that underscores the need for clear communication with patients during the consent process. Despite efforts to anonymize data, AI’s ability to identify individuals presents a significant privacy threat. This challenge is compounded by the dynamic nature of AI, which continuously evolves and uses data in novel ways. Consequently, the consent process must be equally dynamic, enabling patients to reassess and modify their consent as AI systems and their applications change. The rapid advancements in AI technology have outpaced current regulatory frameworks, necessitating updated regulations prioritizing patient agency and consent. This could involve implementing technologically facilitated recurrent informed consent mechanisms for new data uses, thereby respecting patients’ privacy and agency in the face of AI’s dynamic nature. Additionally, the development of generative models for creating synthetic patient data has been proposed to mitigate ongoing privacy concerns. Such models would generate data that are not linked to actual individuals, allowing for the benefits of machine learning without the risks associated with using actual patient data [1,2,22,38].

5.5.2. Ensuring Fairness and Clarity in AI Decision-Making for Healthcare

The potential for biases in AI models, often resulting from unrepresentative data, highlights the critical need to train AI algorithms on diverse and comprehensive datasets. Such measures are necessary to prevent biases affecting patient care and decision-making. Alongside the issues of bias, transparency, and explainability in AI systems, these are of paramount importance. Both patients and healthcare providers frequently encounter difficulties in understanding the decision-making processes of AI systems. Enhancing the interpretability of these systems is essential, enabling patients to make truly informed decisions regarding their care. AI’s ‘black-box’ nature, which obscures its inner workings, poses a significant challenge, affecting the level of trust and undermining the foundation of informed consent [2,38].

5.5.3. Balancing AI Integration with Patient Autonomy and Data Security in Healthcare

Furthermore, the trustworthiness of AI applications is a cornerstone for their successful integration into healthcare. An over-reliance on AI could reduce direct interactions between healthcare professionals and patients, which may adversely affect the quality of care and compromise patient autonomy [2]. This concern is exacerbated by the proliferation of the AI-driven Internet of Things (IoT) in healthcare, which results in the collection of extensive patient data, thereby increasing the risk of privacy breaches and unauthorized data exploitation. Patients must be adequately informed about these risks and the proactive measures implemented to protect their data, including addressing the security vulnerabilities associated with IoT devices [22].

5.5.4. Evolving Consent and Education Strategies for AI and IoT in Healthcare

The potential for reidentification from anonymized data, as highlighted by research, represents a significant privacy risk that must be addressed within the informed consent process. As AI and IoT technologies continue to evolve, it is crucial that the consent process also adapt, becoming a continuous dialogue that allows patients to reassess their participation as technologies advance. The complexity of AI-driven IoT challenges patient autonomy and trust, underscoring the need for a comprehensive approach to patient education and consent. This approach should ensure that patients are well informed about the security measures in place, such as well-defined architecture standards and identity management systems, to safeguard their data and privacy [22,38].

5.5.5. Navigating Intellectual Property and Transparency in AI Healthcare Consent

Moreover, the transparency of AI systems is affected by issues surrounding intellectual property (IP) rights, which can impact the level of insight patients have into the AI systems involved in their healthcare. Patients should be aware of how IP considerations could potentially obscure the workings of AI systems, affecting the care they receive. The dynamic nature of AI algorithms necessitates that informed consent be treated as an ongoing process, with patients allowed to regularly review and renew their consent in line with the evolution of AI applications in healthcare [38].

Engagement and education are critical to informed consent. Both healthcare professionals and patients should be actively involved in the development and application of AI systems. Education about the capabilities and limitations of AI is essential to ensuring that consent is genuinely informed. Integrating AI into healthcare demands a dynamic, transparent, and informed approach to patient consent. This approach must tackle AI biases, protect privacy, enhance transparency and explainability, preserve the clinician-patient relationship, adapt consent processes, and establish robust regulatory and accountability frameworks [2,38].

5.5.6. Dynamic Consent and Security in the Age of AI-Enhanced Healthcare

The continuous and dynamic nature of AI systems, which learn and adapt over time, necessitates an equally flexible and responsive consent process. Patients should receive regular updates on the capabilities and limitations of the AI systems involved in their care, ensuring that their consent is informed and reflective of the latest developments. Such a dynamic consent process is vital for preserving patient autonomy and fostering trust in healthcare systems integrating AI technologies. Concerns regarding equity and bias in AI systems are integral to the informed consent dialogue. Patients should be informed about the potential for AI systems to exhibit biases based on the data they are trained on, which could adversely affect patient care and outcomes. Patients need to understand the proactive steps to ensure that AI systems operate fairly and without prejudice, thereby safeguarding the quality of care for all individuals. Security measures are another critical aspect of AI in healthcare that must be transparently communicated to patients. They should be aware of the robust security protocols to protect their health data, including the potential risks of data breaches and the strategies to prevent them. This communication should extend to the specific security vulnerabilities associated with IoT devices and the measures implemented to mitigate such risks [2,22,38].

The integration of AI in healthcare brings forth a need for adaptive regulatory frameworks and redefined patient consent processes. These changes are essential to address the ethical, legal, and practical challenges posed by the use of advanced AI technologies in healthcare settings, ensuring that patient rights are protected and informed consent processes are adequate in the era of AI. Incorporating these concepts into the discussion on patient rights and informed consent in AI healthcare will provide a more comprehensive and nuanced understanding of the challenges and requirements in this evolving field. It underscores the need for healthcare systems to develop adaptive regulatory frameworks and dynamic, informed consent processes that are responsive to the unique attributes of AI,

such as algorithmic transparency, the ability of machine learning systems to evolve, and the continuous engagement and education of healthcare professionals and patients [1,2,22,38].

6. Limitations

This literature review, while comprehensive, acknowledges certain limitations that merit attention. A primary constraint is the rapid pace of advancements in Artificial Intelligence, which may have led to new developments postdating the studies reviewed. Despite their potential, key technologies, such as Homomorphic Encryption and Differential Privacy, face limitations like computational overhead and compromised utility or accuracy, necessitating ongoing research to refine these methods. A significant challenge in the AI healthcare domain is detecting and mitigating biases. While promising, current techniques require further innovation and tailoring to suit the unique healthcare context. The literature lacks in-depth studies evaluating the real-world effectiveness of various Privacy-Preserving Machine Learning (PPML) techniques within healthcare settings. This gap underscores the need for empirical research to validate these methods in practical scenarios. Furthermore, exploring AI's ethical and legal implications in healthcare, particularly concerning privacy, data protection, and algorithmic discrimination, is not exhaustive. There is a notable deficiency in studies that delve into the perspectives of patients and healthcare professionals on AI and privacy, which are crucial for shaping informed and responsive policies. This review also identifies a need for standardized frameworks for assessing healthcare AI systems' privacy and security, pointing to a need for more structured evaluation methods. Additionally, the research does not extensively cover potential vulnerabilities and threats to privacy in AI-driven healthcare systems. This area is critical, given the sensitivity of healthcare data and the potential consequences of breaches. Lastly, there is a requirement for more interdisciplinary research efforts. These efforts are essential for a holistic understanding of and addressing the multifaceted challenges AI poses in healthcare. While this review synthesizes critical studies on the responsible integration of AI in healthcare, it also highlights substantial knowledge gaps. Areas like the real-world effectiveness of PPML, privacy and ethics implications, patient and healthcare professional perspectives, standardized evaluation frameworks for privacy and security, examination of vulnerabilities, and interdisciplinary research strategies are pivotal. Addressing these gaps through collaborative and comprehensive research is imperative for guiding the responsible integration of AI in healthcare.

7. Future Research in AI-Driven Healthcare

In the evolving realm of AI-driven healthcare, significant emphasis is placed on transforming traditional patient rights and informed consent models. The authors of [2,30] highlight the necessity of redefining the informed consent process, tailoring it to the unique complexities introduced by AI. This includes addressing aspects such as algorithmic transparency, data usage, and the evolving nature of machine learning systems. A dynamic consent model is required, allowing patients to reassess their participation as AI systems evolve continuously. Ensuring a comprehensive understanding and ongoing consent is essential to maintaining patient autonomy and trust in AI-integrated healthcare systems. This shift is vital to tackle the ethical, legal, and practical challenges of advanced AI technologies in healthcare, safeguarding patient rights in this new era.

Concurrently, it is essential to conduct future research in AI-driven healthcare to tackle its varied challenges. A key focus is the development of hybrid privacy-preserving techniques, integrating methods like Homomorphic Encryption for encrypted data computation and Differential Privacy for individual privacy protection. The goal is to refine these methods to balance confidentiality, accuracy, and utility. Another significant area is advancing bias detection and mitigation techniques, which must be sophisticatedly integrated throughout the AI development pipeline. This includes stages from initial data collection to continuous post-deployment monitoring. Creating advanced methods for effective bias detection and mitigation is critical to ensuring equitable and unbiased AI applications in

healthcare. Additionally, the effectiveness of AI explainability interfaces and transparency measures requires thorough evaluation through empirical research. This research should determine how these measures enhance understanding and trust among patients and healthcare providers, utilizing diverse methodologies such as surveys, interviews, and clinical implementations. These efforts are vital to demystifying AI processes for end-users and building a trustworthy AI framework in healthcare.

Examining the unintended consequences of AI governance and regulatory frameworks is also paramount. Research in this area should scrutinize the impact of these frameworks on various facets, including innovation, healthcare costs, access to care, and health disparities. Such an examination is essential to developing evidence-based policies that guide the responsible use of AI in healthcare without stifling innovation or inadvertently widening healthcare disparities. Decentralized data management approaches, like Federated Learning, offer promising avenues for enhancing data security, scalability, and access control in healthcare AI. Investigating these approaches could significantly improve how healthcare data are managed and utilized, mitigating the risks associated with centralized data storage systems. The advancement of techniques for generating synthetic health data and evaluating their applications in tasks like external model validation, benchmarking, and dataset augmentation is another crucial area for exploration. Such advancements could open avenues for accessing diverse and high-quality training datasets, which are fundamental for developing robust and effective AI models in healthcare.

Moreover, understanding the diverse perspectives of patients and healthcare professionals on AI integration in healthcare is vital. Public dialogues and surveys should be conducted to gain insights into these groups' views, particularly regarding privacy, discrimination, dignity, and trust. This understanding should inform the development and implementation of AI technologies in healthcare. There is also a need to institute responsible data practices and develop novel AI evaluation metrics focused on fairness and accountability. This includes establishing collaborative benchmark dataset initiatives and forming interdisciplinary research teams, including ethicists and social scientists, to ensure a holistic approach to AI integration in healthcare. Lastly, developing education programs to enhance AI literacy and ethics competencies among healthcare professionals is essential. Such programs will ensure a well-informed workforce capable of integrating AI responsibly into healthcare practices, bridging the gap between technological advancements and clinical applications. This comprehensive roadmap for future research underscores the importance of a multifaceted and interdisciplinary approach to integrating AI into healthcare. It highlights the need for continuous innovation, ethical consideration, and rigorous evaluation to realize the full potential of AI in enhancing healthcare outcomes while safeguarding patient welfare and rights.

8. Conclusions

The integration of Artificial Intelligence (AI) in healthcare transcends the realms of technology, delving into profound moral and ethical considerations. Our research highlights that incorporating AI in healthcare is not merely about harnessing technological prowess but also about navigating the complex ethical landscape accompanying it. This calls for a holistic approach that harmoniously aligns technical advancements with deep-rooted ethical principles. AI's potential to revolutionize healthcare is undeniably vast, offering groundbreaking improvements in patient care, diagnosis, treatment, and overall healthcare management. However, with this remarkable potential comes a weighty responsibility: ensuring that AI's integration into healthcare systems upholds the highest ethical standards. It is imperative to consider the efficiency and effectiveness of AI and its applications' moral implications, particularly in sensitive areas like patient data handling and decision-making processes.

Blockchain technology emerges as a promising component within this broader context. Its capabilities in enhancing data security and ensuring transparency are noteworthy. However, it is crucial to recognize that blockchain is just one element within a larger, more

complex ecosystem of solutions required to address the multifaceted challenges posed by AI. These challenges include mitigating algorithmic bias, which can perpetuate existing inequalities or introduce new ones; ensuring privacy in an age where data are invaluable and vulnerable; and maintaining autonomy, especially in clinical decision-making contexts where AI systems might influence or dictate patient care decisions.

Moreover, the call for transparent, explainable AI systems cannot be overstated. The ‘black box’ nature of some AI algorithms, where the decision-making process is opaque and difficult to understand, poses significant challenges. This lack of transparency hampers trust in AI systems and complicates ethical evaluations and accountability in healthcare decision-making. Thus, developing AI systems that are not only technically proficient but also explainable and understandable to a wide range of users, including healthcare professionals and patients, is essential. Such transparency is vital to building trust, fostering informed decision-making, and ensuring that AI systems are used responsibly and ethically.

Equally important is the involvement of diverse stakeholders in the conversation about AI in healthcare. This includes technologists, healthcare providers, ethicists, and patients, who are the ultimate beneficiaries of these technologies. Engaging a wide range of perspectives is crucial to understanding AI’s real-world implications, concerns, and expectations in healthcare. It ensures that the development and deployment of AI technologies are grounded in the realities of patient needs and experiences, thereby promoting patient-centered innovation. This inclusive approach is fundamental to ensuring that AI serves the entire healthcare community’s diverse needs and respects all individuals’ values and dignity.

Integrating AI in healthcare is a journey that intertwines technological innovation with ethical and moral responsibility. It demands careful consideration, collaborative effort, and a steadfast commitment to ethical principles to realize the full potential of AI in enhancing healthcare while safeguarding the core values of trust, privacy, autonomy, and equity. The path forward for AI in healthcare is one of cautious but optimistic advancement. The challenges identified in our research are substantial but not insurmountable. Future research should focus on advancing the development of ethical AI frameworks, exploring new privacy-preserving technologies, and enhancing methods for detecting and mitigating algorithmic bias. Additionally, there is a critical need for dynamic regulatory frameworks that can adapt to the rapid pace of technological innovation in AI. Collaborative efforts across various sectors, including technology, healthcare, ethics, and policy-making, are imperative to effectively navigate the complexities of AI integration in healthcare. The ultimate goal is to harness AI’s transformative power to benefit patient care while diligently safeguarding patient rights and promoting equitable healthcare practices. As AI continues to evolve, our commitment to these principles will ensure its role as a benevolent force in healthcare.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Murdoch, B. Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era. *BMC Med. Ethics* **2021**, *22*, 122. [[CrossRef](#)] [[PubMed](#)]
2. Reddy, S.; Allan, S.; Coghlan, S.; Cooper, P. A Governance Model for the Application of AI in Health Care. *J. Am. Med. Inform. Assoc.* **2019**, *27*, 491–497. [[CrossRef](#)] [[PubMed](#)]
3. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.; Akl, E.A.; Brennan, S.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Br. Med. J.* **2021**, *372*, n71. [[CrossRef](#)] [[PubMed](#)]
4. Morley, J.; Machado, C.C.V.; Burr, C.; Cowls, J.; Taddeo, M.; Floridi, L. The Debate on the Ethics of AI in Health Care: A Reconstruction and Critical Review. *Soc. Sci. Res. Netw.* **2019**. [[CrossRef](#)]
5. Prakash, S.; Balaji, J.N.; Joshi, A.; Surapaneni, K.M. Ethical Conundrums in the Application of Artificial Intelligence (AI) in Healthcare—A Scoping Review of Reviews. *J. Pers. Med.* **2022**, *12*, 1914. [[CrossRef](#)]

6. Biller-Andorno, N.; Ferrario, A.; Jöbges, S.; Krones, T.; Massini, F.; Barth, P.; Arampatzis, G.; Krauthammer, M. AI Support for Ethical Decision-Making around Resuscitation: Proceed with Care. *Medrxiv (Cold Spring Harb. Lab.)* 2020, preprint. [CrossRef]
7. Wang, C.; Zhang, J.; Lassi, N.; Zhang, X. Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. *Healthcare* **2022**, *10*, 1878. [CrossRef]
8. Panagopoulos, A.; Minssen, T.; Sideri, K.; Yu, H.; Compagnucci, M.C. Incentivizing the Sharing of Healthcare Data in the AI Era. *Comput. Law Secur. Rev.* **2022**, *45*, 105670. [CrossRef]
9. Khalid, N.; Qayyum, A.; Qayyum, A.; Al-Fuqaha, A.; Qadir, J. Privacy-Preserving Artificial Intelligence in Healthcare: Techniques and Applications. *Comput. Biol. Med.* **2023**, *158*, 106848. [CrossRef]
10. Zarifis, A.; Kawalek, P.; Azadegan, A. Evaluating If Trust and Personal Information Privacy Concerns Are Barriers to Using Health Insurance That Explicitly Utilizes AI. *J. Internet Commer.* **2020**, *20*, 66–83. [CrossRef]
11. Richardson, J.W.; Smith, C.; Curtis, S.; Watson, S.E.; Zhu, X.; Barry, B.A.; Sharp, R.R. Patient Apprehensions about the Use of Artificial Intelligence in Healthcare. *Npj Digit. Med.* **2021**, *4*, 140. [CrossRef] [PubMed]
12. Pereira, T.; Morgado, J.; Silva, F.; Pelter, M.M.; Dias, V.; De Cássia Nogueira Barros, R.; De Freitas, C.; Negrão, E.; De Lima, B.F.; Da Silva, M.C.; et al. Sharing Biomedical Data: Strengthening AI Development in Healthcare. *Healthcare* **2021**, *9*, 827. [CrossRef] [PubMed]
13. Rahman, A.; Hossain, M.S.; Muhammad, G.; Kundu, D.; Debnath, T.; Rahman, M.S.; Khan, M.S.I.; Tiwari, P.; Band, S.S. Federated Learning-Based AI Approaches in Smart Healthcare: Concepts, Taxonomies, Challenges and Open Issues. *Clust. Comput.* **2022**, *26*, 2271–2311. [CrossRef] [PubMed]
14. Elhoseny, M.; Haseeb, K.; Shah, A.A.; Ahmad, I.; Jan, Z.; Alghamdi, M.I. IoT Solution for AI-Enabled PRIVACY-PREserving with Big Data Transferring: An Application for Healthcare Using Blockchain. *Energies* **2021**, *14*, 5364. [CrossRef]
15. Alabdulatif, A.; Khalil, I.; Rahman, M.S. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. *Appl. Sci.* **2022**, *12*, 11039. [CrossRef]
16. Ali, S.; Abdullah; Armand, T.P.T.; Athar, A.; Hussain, A.; Ali, M.; Muhammad, Y.; Joo, M.-I.; Kim, H.C. Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. *Sensors* **2023**, *23*, 565. [CrossRef] [PubMed]
17. Shinde, R.; Patil, S.; Kotecha, K.; Ruikar, K. Blockchain for Securing AI Applications and Open Innovations. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 189. [CrossRef]
18. Tagde, P.; Tagde, S.; Bhattacharya, T.; Tagde, P.; Chopra, H.; Akter, R.; Kaushik, D.; Rahman, M.H. Blockchain and Artificial Intelligence Technology in E-Health. *Environ. Sci. Pollut. Res.* **2021**, *28*, 52810–52831. [CrossRef]
19. Xu, J.; Glicksberg, B.S.; Su, C.; Walker, P.B.; Bian, J.; Wang, F. Federated Learning for Healthcare Informatics. *J. Healthc. Inform. Res.* **2020**, *5*, 1–19. [CrossRef]
20. Munjal, K.; Bhatia, R. A Systematic Review of Homomorphic Encryption and Its Contributions in Healthcare Industry. *Complex Intell. Syst.* **2022**, *9*, 3759–3786. [CrossRef]
21. Mosaiyebzadeh, F.; Pouriye, S.; Parizi, R.M.; Sheng, Q.Z.; Han, M.; Zhao, L.; Sannino, G.; Ranieri, C.M.; Ueyama, J.; Batista, D.M. Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey. *Electronics* **2023**, *12*, 2703. [CrossRef]
22. Keshta, I. AI-Driven IoT for Smart Health Care: Security and Privacy Issues. *Inform. Med. Unlocked* **2022**, *30*, 100903. [CrossRef]
23. Olatunji, I.E.; Rauch, J.; Katzensteiner, M.; Khosla, M. A Review of Anonymization for Healthcare Data. *Big Data* **2022**. [CrossRef]
24. Angerschmid, A.; Zhou, J.; Theuermann, K.; Chen, F.; Holzinger, A. Fairness and Explanation in AI-Informed Decision Making. *Mach. Learn. Knowl. Extr.* **2022**, *4*, 556–579. [CrossRef]
25. Formosa, P.; Rogers, W.; Bankins, S.; Griep, Y.; Richards, D. Medical AI and Human Dignity: Contrasting Perceptions of Human and Artificially Intelligent (AI) Decision Making in Diagnostic and Medical Resource Allocation Contexts. *Comput. Hum. Behav.* **2022**, *133*, 107296. [CrossRef]
26. Kudina, O. Regulating AI in Health Care: The Challenges of Informed User Engagement. *Hastings Cent. Rep.* **2021**, *51*, 6–7. [CrossRef] [PubMed]
27. Meskó, B.; Topol, E.J. The Imperative for Regulatory Oversight of Large Language Models (or Generative AI) in Healthcare. *Npj Digit. Med.* **2023**, *6*, 120. [CrossRef]
28. Vaassen, B. AI, Opacity, and Personal Autonomy. *Philos. Technol.* **2022**, *35*, 88. [CrossRef]
29. Kelly, C.; Karthikesalingam, A.; Suleyman, M.; Corrado, G.S.; King, D. Key Challenges for Delivering Clinical Impact with Artificial Intelligence. *BMC Med.* **2019**, *17*, 195. [CrossRef]
30. Tom, E.S.; Keane, P.A.; Blazes, M.; Pasquale, L.R.; Chiang, M.F.; Lee, A.; Lee, C.S. Protecting Data Privacy in the Age of AI-Enabled Ophthalmology. *Transl. Vis. Sci. Technol.* **2020**, *9*, 36. [CrossRef]
31. Schiff, D.; Borenstein, J. How Should Clinicians Communicate with Patients about the Roles of Artificially Intelligent Team Members? *AMA J. Ethics* **2019**, *21*, E138–E145. [CrossRef]
32. Finck, M. *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?* Panel for the Future of Science and Technology (STOA), Directorate-General for Parliamentary Research Services (EPRS) European Parliament: Brussels, Belgium, July 2019. PE 634.445. Available online: <https://data.europa.eu/doi/10.2861/535> (accessed on 15 November 2023).

33. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain Technology Applications in Healthcare: An Overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [[CrossRef](#)]
34. Lysaght, T.; Lim, H.Y.; Xafis, V.; Ngiam, K.Y. AI-Assisted Decision-Making in Healthcare. *Asian Bioeth. Rev.* **2019**, *11*, 299–314. [[CrossRef](#)] [[PubMed](#)]
35. Bankins, S.; Formosa, P.; Griep, Y.; Richards, D. AI Decision Making with Dignity? Contrasting Workers' Justice Perceptions of Human and AI Decision Making in a Human Resource Management Context. *Inf. Syst. Front.* **2022**, *24*, 857–875. [[CrossRef](#)]
36. Sidebottom, R.; Lyburn, I.; Brady, M.; Vinnicombe, S. Fair Shares: Building and Benefiting from Healthcare AI with Mutually Beneficial Structures and Development Partnerships. *Br. J. Cancer* **2021**, *125*, 1181–1184. [[CrossRef](#)]
37. Han, H.; Liu, X. The Challenges of Explainable AI in Biomedical Data Science. *BMC Bioinform.* **2021**, *22* (Suppl. S12), 443. [[CrossRef](#)]
38. Bernal, J.; Mazo, C. Transparency of Artificial Intelligence in Healthcare: Insights from Professionals in Computing and Healthcare Worldwide. *Appl. Sci.* **2022**, *12*, 10228. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.