Navigating Ethics and Regulation in AI Health Cloud: Challenges and Opportunities for United States Healthcare

Oluwasanya Luke Ogunsakin[1]; Kevin Mukasa[2]

[1]Bournemouth University; [2]Maharishi International University

Publication Date: 2026/01/19

Abstract: This paper explores the social issues, ethical and compliance concerns relating to the implementation of AI-driven health cloud technologies in the United States. It tries to figure out how regulations, ethics and stakeholder trust are set up even in case they are unpredictable and examines innovation and value creation opportunities. In theory, the study is a synthesis of the literature available on the subject that identifies the key advantages and limitations of AI health cloud application. The advantages include more transparent clinical processes, more accurate surveillance of the health of the population, and more responsive individual treatment. The key issues are ambiguous legal standards, ethical and regulatory breaches, the lack of patient control over information, and poor privacy. The paper finds that U.S. AI health cloud programs need to integrate innovation and compliance, and advocate policy reforms that would align ethics, regulations, and compliance. It calls to action the inclusion of ethics and compliance to spur policy change in the U.S. AI cloud space. The research recommends that policymakers in health systems and leaders should work together to develop meaningful, moral, and viable policies.

Keywords: *AI Health Cloud, Ethics, Regulation, Innovation in Healthcare, Governance and Digital Health.*

How to Cite: Oluwasanya Luke Ogunsakin; Kevin Mukasa (2026) Navigating Ethics and Regulation in AI Health Cloud: Challenges and Opportunities for United States Healthcare. *International Journal of Innovative Science and Research Technology*, 11(1), 942-952. https://doi.org/10.38124/ijisrt/26jan367

I. INTRODUCTION

Within the healthcare sector, the influence of Artificial Intelligence (AI) and wireless computing has changed the way medical information is stored and used clinically. However, technological advancements in the health sector have raised concerns relating to the privacy and accountability of patient data, legal compliance within the system, as well as the ownership of system data (Agapito & Cannataro, 2023). It is, therefore, a question of ‘how’, and not, ‘if’, healthcare institutions within the United States will adopt AI-enabled cloud computing which has incredibly tight ethical and legal boundaries pertaining to the use of AI technology (Yandrapalli & Sharma, 2025).

The use of AI and cloud computing in healthcare comes with improvements to health services operations, real-time data analytics, and the use of advanced cloud computing analytics, especially in unserved areas (Saratkar & Langote, 2023). On the other hand, the possibility of legal data breach, reputational damage, and loss of data custody remain critical risks. For instance, the capability to store and jointly analyze data from over multiple global sites of multicenter clinical trials provides cloud computing to health organizations (Gomase et al., 2025). This also raises cross-border issues of varying data use and patient consent of complex data-privacy restrictions. Furthermore, deploying reinforcement deep learning in real-time responsive healthcare using cloud and edge healthcare infrastructure raises concerns over mesh ethics (Du et al., 2024). This is more so where the automated decision to dispense healthcare services interfaces with the clinical judgement of the decision maker.

Like the Health Insurance Portability and Accountability Act (HIPAA) in the US, no concern is made for the continuously educating and evolving AI-driven Cloud Systems. This creates a regulatory lag, where the anticipated legal protections fall considerably short when compared to the technological advancements (Babalola et al, 2024). A case in point is the HIPAA which provides the legal framework to protect certain PII health records but is mute on the unethical use of predictive analytics and generative AI on downstream decision-making and its application in the healthcare domain (Ali & Aysan, 2025). Similarly, on a daily basis, the Office of the Food and Drug Administration (FDA) is faced with the oversight of medical devices which incorporate AI, the algorithms of which shift and develop even after the devices have been approved for use (Du et al., 2024). This vexation creates a 'catch 22' scenario for practitioners in the domain of healthcare who wish to progress, and those who wish to adhere to regulations (Sonani and Govindarajan 2025).

In the region, the paradox of accountability structures in multi-stakeholder contexts continues to emerge as a governance concern. As Agapito and Cannataro (2023) describe, cloud healthcare systems comprise interconnectedness of hospitals, cloud vendors, AI developers, and regulators. Data discrimination in the algorithms and breach of accountability are legal and ethical responsibilities. As Babalola et al. (2024) describe, without governance models, violations of compliance and public trust are commonplace. Discriminatory AI issue diagnostics, carelessly used in healthcare systems, and worst of all, Ap system AI, created conditions of legal, financial, and reputational exposure for healthcare institutions (Du et al., 2024). This, however, illustrates very poorly the extent to which empirical evidence relates to regulation, ethics, and the technology of an innovation.

Generally, it seems scholarly works have been carried out on the use of clouds in e-health computing in the e-health sector than in other disciplines. For example, Georgiou and Lambrinoudakis (2020) viewed cloud frameworks in Europe concerning e-health security and the clouds concerning the need for policy frameworks. Similarly, Singh (2023) analyzed the regulatory constraints in AI-driven healthcare systems and discussed the paradox of innovation and regulation. However, despite these efforts, the body of work is still lacking in its attempts to synthesize the ethical issues, regulatory issues, and technological instruments. Moreover, the works on the military (Rangel, 2021) and governance (Lichtenheim, 2024) regarding the integration and control of tertiary cloud systems lack in healthcare insight primarily because the frameworks fail to address fundamental patient rights and ethical issues of care.

To fill in these and other gaps, this research, "Navigating Ethics and Regulation in AI Health Clouds: Challenges and Opportunities for U.S. Healthcare", aims to investigate the nexus of the technological feasibility, the ethical concerns, and the legal barriers.

To accomplish this, the research was qualitative in nature and reviewed various academic articles, research studies, and policy papers that were published between the years 2020 and 2025. The review was an integration of evidence in various disciplines such as healthcare, artificial intelligence, cloud computing, ethics and law. This method has explained the interaction between technology, regulation and adoption in the U.S. healthcare system. The conceptual framework was based on the major ideas of the reviewed studies and policy documents. It was concerned with identifying the core drivers, issues, and opportunities that determine the ethical application of AI health cloud services within the U.S. healthcare industry and revealing why the country is ahead of the pack in this domain over most of its counterparts.

- *Conceptual Framework*

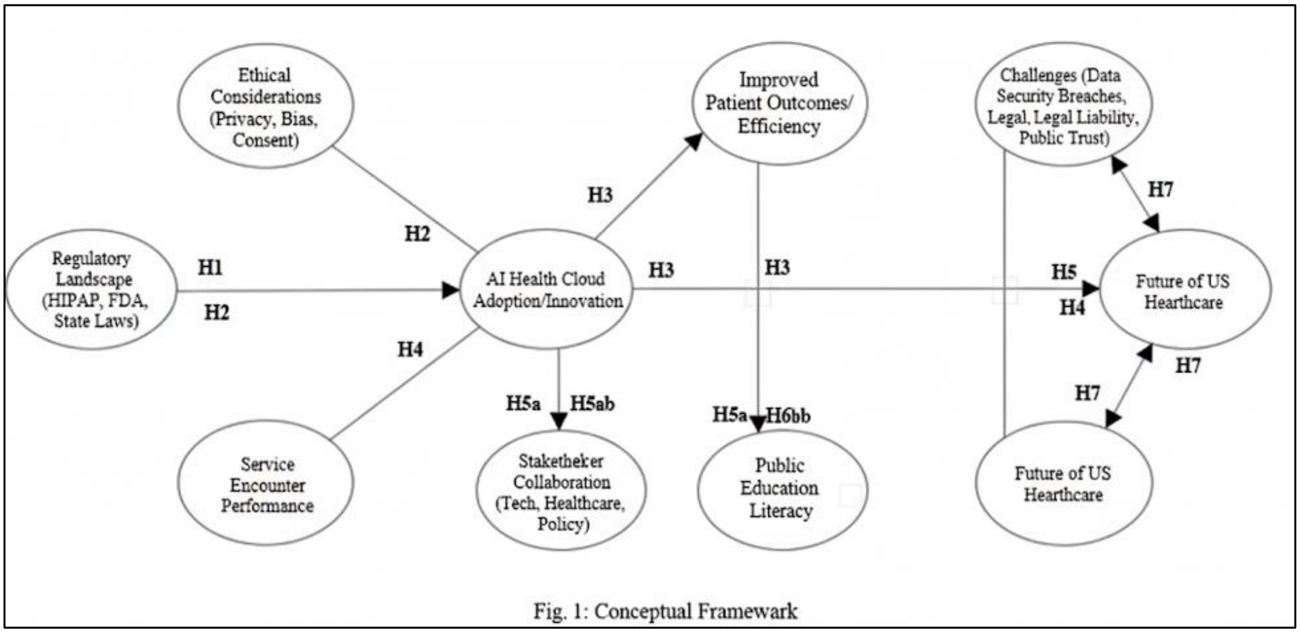
Ethical Considerations (Privacy, Bias, Consent)
Improved Patient Outcomes/ Efficiency
Challenges (Data Security Breaches, Legal, Legal Liability, Public Trust)
H3
H7
H2
Regulatory Landscape (HIPAP, FDA, State Laws)
H1
H2
AI Health Cloud Adoption/Innovation
H3
H3
H5
H4
Future of US Hearthcare
H4
H7
H7
H5a
H5ab
H5a
H6bb
Service Encounter Performance
Stakethe ker Collaboration (Tech, Healthcare, Policy)
Public Education Literacy
Future of US Hearthcare

Fig. 1: Conceptual Framewark

Source: Author's conceptual framework, adapted from existing studies on AI, cloud computing, and healthcare regulation.

Fig 1 illustrates a mix of governance, ethics, technology, and stakeholders that affects the deployment and growth of cloud-based AI in US healthcare. This model places the adoption/ innovation of AI-health cloud systems in the center of the figure and describes the governance, ethics and policy service performance tiers in the multi-dimensional constellation of health outcomes, stakeholder synergies, education and barriers, and the future of the U.S. health care system.

The landscape of adoption and use comes forth as the foremost imperative. The U.S. Health Insurance portability and accountability act (HIPAA) and the federal Food and Drug Administration (FDA) regulation and a number of state legislations under them, at the same time, grant and withhold scads of opportunities to cloud-based health systems. There is a view that the absence of clear and enforceable adoptions rules, anticipating overregulated and expensive compliance, will in reality thwarts adoptions (Singh, 2023; Babalola et al, 2024). This, in totality, indicates that the H1 and H2 hypotheses portray paradox in regulation that in one part, enables the U.S. AI health cloud adoption in healthcare, while in the other, constrains it.

Besides the legal aspects, the ethical issues of privacy and data protection, as well as the ability to withdraw consent, impact the core parameters of 'acceptance'. Trust of patients in AI systems on the cloud relies heavily on the answers the providers give regarding data bias and 'black box' algorithms. Unsolved ethical problems, especially those regarding Generative AI, are counter to the trust in digital health technologies (Ali and Aysan, 2025). In support of this, Agapito and Cannataro (2023) claim that ethical chapters should be integrated with the digital cloud to sustain responsibly advanced technology. Thus, H2 articulates the understanding that ethical issues are not merely difficult external issues; they are major factors regarding the speed and direction of adoption of AI health cloud.

Furthermore, the adoption and the service performance of the encounter depict the same phenomenon, as the service impact framework also illustrates. The service encounters, or the interactivity of the triad of patients, clinicians and AI-enabled platforms, construction does impact the experiential use and perceptions of the technology. AI health cloud systems are adopted more rapidly in cases where such systems enhance the accuracy of diagnoses, the workflow of clinicians, or the experiences of patients (Du et al., 2024). In contrast, poor usability, excessive workloads, or the misalignment with real clinical practice can also lead to technophobia. This also goes in line with the literature that states that the successful adoption of technology is not the problem with technology. It is about how the service delivery systems incorporate the technology (Saratkar & Langote, 2024).

As indicated in (H3), the predictive analytics outcomes in AI health cloud systems will be improved with the expansion of the analytics and collaborative functionality. Gomase et. al (2025) associates the augmenting of cloud-based systems with the near real-time observation and increased productivity of the execution of the clinical health care delivery systems. This is based on the factors of (H5a) systemize stakeholder integration and cooperation, and the discourse of the populace's digital literacy and education (H6b) level. As such, there is need for collaboration among the technology developers, health care institutions and policy makers to avoid fragmentation of innovations (Sonani & Govindarajan, 2025). Discourse on education is equally relevant, where the technology will be misused and abused by patients and staff and eventually the outcomes will be disappointment (Lichtenheim, 2024).

The digital world can be detrimental or hostile to an organisation due to something like a negative perception from the public or even a data or information security breach. H5 and H7 describe barriers in the model as critical, tiered, and interrelated. Singh (2023) points out the contradiction of compliance versus trust as the more institutionalized approach to framing security exposure. The counter scheme of the redesign of public trust and the litigation of the backlogged risk spectrum contradict the orderless range of innovation. On the other hand, under the right conditions, the problems can be resolved and give rise to a more reliable and robust digital health system (Georgiou & Lambrinoudakis, 2020).

In the same vein, the multi-dimensional inter-dependent criteria of the U.S. health system and the remaining predictors portray the rest of the world as the most sophisticated forecast of the system in the hands of a single country (Yandrapalli, 2025). This situation requires a balanced optimization of compliance, ethical advocacy, risk harnessing, and systematized governance in the domain. If such modalities are implemented, the U.S. health system stands to gain from the predicted operational explosion of the health cloud AI (Rangel, 2021). On the other hand, the absence of ethical compliance leaves the governance and trust framework governance as a significant risk and undermines the sector's longevity (Yandrapalli, 2025).

II. LITERATURE REVIEW

The subsequent section reviews literature related to this study.

➢ *Ethical Performance in AI Health Cloud*

As far as ethical performance within AI health cloud systems is concerned, it has to do with the emerging systems value of transparency, equity, and the autonomous will of the patients. Yandrapalli (2025) observes that within the folds of the US healthcare system ethics, wherein sensitive and guarded patient information, the ethics performance outcome has outcome determinative effect on the level of adoption. Singh

(2023) emphasizes the sensitive character of the medical domain. Yandrapalli (2025) further posits that medical data is of such a character that its ethical safeguards against misuse, discrimination, and erosion of trust in medical records are misplaced. In the same vein, directed Bouderhem (2024) also argues that the ethical performance gap in the design stage of AI health cloud systems. It has been a barrier to the socio-ethical acceptability of systems within which patients are cloud diagnosed, treated, and prognosticated. Their views are in alignment with the study of Murphy, Murphy and Sowe (2021) who argue that health AI has to earn the title by abiding to ethical data fairness and stewardship as primary ratios of the AI transaction to achieve socio-ecological sustainability.

Karimian, Petelos, and Evers (2021) explain that failing to view the data in an ethical context can have negative consequences, including dense decision making, problematic and biased automated decision processes that deepen inequalities and further marginalize the most vulnerable groups of any society. Martinez-Martin et al. (2021) document Orwellian applications of ‘caring’ technologies that lack the rudiments of informed consent and the use of certain ambient intelligence systems in healthcare. In the US, the intersection of healthcare inequity, a multi-layered and oftentimes obscured challenge, with so-called ‘trickster’ ethical perspectives tends to amplify negative sentiments amongst the patient and provider population. Moreover, Kokala (2022) has heads that explainable AI might be useful to the ethical problems of over-simplification and lack of transparent explainability. Based on this, Palaniappan, Lin and Vogel (2024) avowed that AI has the potential to clarify the complex reasonings of decision-making and of its processes, and hence, clarify the reasoning to the users, patients and clinicians, of the AI-suggested decisions.

As Ali and Aysan (2025) have argued, ethical misconceptions may, in fact, skew and falsely guide the discourse around generative AI systems in the Cloud integrated healthcare systems. This sentiment is echoed by Amugongo et al. (2025) who view the ethics of AI ‘operationalized’ with ‘agile’ systems of development and real-time ‘ethics in the ink’ of continuous compliance systems as dynamically adjustable on the fly. In these contexts, Yandrapalli and Sharma in the paper ‘The Trouble with Ethics in Cloud Healthcare’ claim that US healthcare providers have a responsibility to put ethics foremost in the business case for cloud adoption, distinguishing ethics from ancillary considerations. Hence, the use of AI health clouds, ethical conduct is more than just ethical conduct for the sake of it: it determines the trust, clinician engagement, and reputation of the institution.

- *Regulatory Performance and Healthcare Legitimacy*

Regulatory performance pertains to the legal and regulatory requirements of the industry regarding the operation of the AI Health Cloud Systems at the federal and state levels (Ali & Aysan, 2025). In the case of the U. S. legal system, this boils down to HIPAA, FIH obligations regarding AI/ML based medical devices, and other emerging laws like data protection. Due to the fragmentation of the U.S. regulatory system, compliance and the cloud of uncertainty it creates for health care providers is quite alarming (Palaniappan, Lin, and Vogel, 2024). These problems cut across and go beyond the legal sphere, and define what can reasonably be expected of the providers and the patients in relation to the operation of the AI Health Cloud Systems.

As confirmed by Shah and Konda (2022), Saltako et al (2024), and Najana and Ranjan (2024), the process of gaining compliance and trust emerges from the appropriate regulatory compliance steps taken. Audit trails, encryption, and other security certificates should alleviate the concerns of stakeholders in cloud-enabled health care systems. Stakeholders’ reasonable assurance regarding the protection of such sensitive information is a direct outcome of the governance frameworks in place. Najana and Ranjan (2024) do seem to indicate that there might be cloud adoption gaps in the subsectors of health care, which in turn, outlines the system readiness relational of in health care. Flexible compliance, as a genuine modular construct, promises to deliver systems that trigger organizational sanctions for lapse, and which, at a minimum, meets the outer legitimacy criteria for societal, organizational, and regulatory compliance that is increasingly demanded (Karimian, Petelos, and Evers, 2021).

Scholarly works continue to illustrate the evolving nature of the complexities of regulation. According to Prakash et al. (2024), the application of machine learning compliance tools which automatically audit and monitor processes may alleviate some regulatory burdens. Sonani and Govindarajan (2025) outline governance-oriented AI systems that incorporate ethics and regulatory compliance at the design level to facilitate proactive organizational adherence to changing regulatory obligations. Still, Agapito and Cannataro (2023) warn that the compliance burden, along with the system’s design and operational complexities, disproportionately impacts small providers of healthcare services. These works highlight the regulatory outcome contradiction as both an opportunity and a challenge: fundamental to the underpinning of healthcare’s legitimacy, but rather vague, given the legal and technological context.

- *Stakeholder Trust and Resistance to AI Heath Cloud*

Barriers of trust and a patient’s right to privacy and protection, a clinician’s responsibility to a patient’s diagnostic accuracy, and the institution’s assumption about vendor responsibility all need to be resolved. Williamson and Prybutok (2024) note that AI-patient safety and accountability frameworks and control substitutes need to be installed to gain patient trust for the tools to share their sensitive genomic information. Rehan (2023) supportive of this statement uses genomic research to explain this trust paradox. The researcher notes that patients are more likely to provide sensitive data if they are assured of the controlled system data, and the accuracy of the data is warranted. Liaw et al. (2020) affirm that structural trust and control mechanisms are a prerequisite to patient participation and engagement. For the adoption of AI tools, clinicians need to trust that systems will ethically manage their Electronic Health Records to gain confidence. Lack of trust have been identified as the root cause of this resistance.

ML systems are often associated with uncertainties and skepticism, which stems from a breakdown in trust. Distrust in the salespersons and patients alike is widespread for intricate unethical reasons, including a lack of informed consent and blunders in control, as discussed by Prakash et al. (2022). Yadav et al. (2023) argue that breaches of privacy and personal data are more aggressively opposed when associated with opaque or over-surveilling AI systems. Zhang and Zhang (2023) provide similar reasoning by explaining that the suspicion of stakeholders is justified and, when AI is offered, communication about its boundaries and protective pillars is equally necessary. In the U.S, the suspicion of trust is more pronounced when discussed in the context of the public debate regarding algorithmic bias and social responsibility, and can immediately translate to opposition towards adoption (Yadav et al., 2023).

Trust gained from stakeholders will help in reducing conflicts. As Lichtenheim (2024) points out, a way to augment trust is to block the governance frameworks of AI and cloud technology, which streamlines system responsibility. Gomase et al. (2025) argues that, 'global clinical trial platforms are in the forefront of facilitating cloud-based health research in a transparent and ethically accountable manner'. Rangel (2021) further explains that the military's cloud lessons demonstrate how the rigidity of compliance and security can engender institutional trust. Taken together, they offer a paradoxical image: the absence of trust from stakeholders is the overwhelming reason for resistance, while the presence of trust is crucial for adoption.

- *Institutional and Market Barriers as Moderators*

Trust may develop, but there are barriers which still arise to counter the dynamic and limit organizational flexibility. For instance, compliance costs, in particular, certifiable and audit relevant costs, almost invariably confine organizations to a limited set of vendors and, in the process, eliminate the possibilities of a trust relationship (Najana & Ranjan, 2024). Furthermore, Salako et al. (2024) contend that financial and non-financial 'relational' constraints, including vendor lock-in and chronic agreements, diminish the ability of providers to shift to more ethically defensible positions. The outcome is a self-inflicted contradiction where organizational systems are advanced without the relevant consideration of trust, and ethical systems are put in place precisely because it is assumed that the retention costs are more favorable than the ethics in question (Salako et al., 2024).

Take for example the lack of good substitutes and how that worsens the situation. In doing research for Google’s Project Nightingale, Arigbabu et al. (2024) noted how hospitals continued forming ethically questionable partnerships because there were no competitive alternatives that could be considered similarly attractive. This point is also made by Saratkar and Langote (2024) who argue that during the cloud adoption in healthcare, there is a chronic lack of vendors and, therefore, very little competition in the marketplace. These, as noted by Agapito and Cannataro (2023), can self-sustain barriers to cloud dependency within the market, which means that healthcare organizations are targets for unethical cloud deals, readily available from cloud providers, and inefficient cloud deals. These barriers, particularly in the U.S.A. where market technology vendors consolidation is high, provide a structural loss.

On the contrary, some scholars discuss the ways in which certain policies and types of governance may assist in mitigating some of the barriers. Babalola et al. (2024) allot the compliance and accountability as well as the vendor governance to the cloud relational and structural barriers to cloud governance frameworks. Georgiou and Lambrinoudakis (2020) mention the European evidence which shows that certain types of standardization around compliance and security can alleviate the 'as a service' market lock-in phenomenon and enhance competition among the providers. As argued by Du et al. (2024), more advanced scheduling and orchestration systems remove some operational jams which expand the choice of providers that institutions can do business with. The fundamental argument is that the institutional and market barriers are severe. Innovation and reform are ways to show that these barriers are controllable (Babalola et al., 2024).

- *Challenges of Navigating Ethics and Regulation in AI Health Cloud in the United States*

There is a striking regulatory lag in the United States between the speed of AI cloud technological advancement and the capability of current regulatory systems to exercise control. To illustrate, the Health Insurance Portability and Accountability Act (HIPAA) and the Food and Drug Administration (FDA) established guidelines to control the rest of the world’s healthcare and medical instruments, but they have proved inadequate in the application of adaptive, perpetually modifying, cloud-based systems (Singh, 2023). The legislation is fundamentally rigid, focused on legalistic, contractual algorithms reliant on static systems, and is utterly unprepared for technologies that autonomously change after deployment. The regulatory lag sows’ discontent within a legal system, giving rise to multiple paradoxes for hospitals and developers, who are not sure whether their practice is on the right side of the law. In addition to this confusion, there is the separate, deeply fragmented system of governance in the United States. Federal initiatives are tangled up with state privacy laws, creating a double and, in some instances, multiple regulated environments for healthcare systems (Zhang & Zhang, 2025).

As an illustration, a healthcare organization with a presence in both California and Texas would likely have conflicting responsibilities concerning patient consent, data conscription, and data portability, which would place practitioners at a significant risk for legal litigation (Palaniappan, Lin, and Vogel 2024). Compliance costs are especially burdensome for smaller structures which do not possess the financial means or the legal and technical skills required to monitor and resolve divergent legal requirements in different countries (Najana and Ranjan 2024). Consequently, instead of promoting new ideas, the dysfunctional legal system as a whole slows down the process of new idea application and increases the costs associated with their use.

In addition to regulatory vagueness, the U.S. experience with the AI health cloud is profoundly influenced by ethical issues, especially concerning bias, transparency, and consent. Multiple works document that AI systems utilizing U.S. healthcare datasets tend to reinforce structural inequities, especially among racial minorities, women, and impoverished patients (Karimian, Petelos, & Evers, 2022). The inequities embedded within these biased models are likely to be exaggerated as they are distributed via cloud technology multiple health systems, swift falling across frameworks, and incorporated into daily clinical workflows. Transparency in other respects is also disturbing. Many AI software products claimed to be “explainable” in the technical documents fail to offer plausible descriptions that are useful to either clinicians or patients (Zhang & Zhang, 2025). For instance, a probability score of a patient for having to be readmitted to the hospital may be explained and made interpretable, but would be far removed from what a clinician at the bedside would think, or what a regulator trying to ascertain fairness would be looking for (Kokala, 2022). Consent remains a significantly more willful problem. Patients are usually directed to sign documentations of terms of service that are very long and contain technical language that the patients are faced with unreasonable chances of comprehension (Zhang & Zhang, 2025).

As noted by Murphy et al, (2021), consumers are “data subjects” whose data is stored, processed, and reused by multiple vendors for research and commercial purposes, and do not understand the implications that arise from usage of their data. More academics have said that the risks of informed consent in this situation is becoming more superficial, rather than actually protecting patient’s rights (Williamson & Prybutok, 2024). Failure to “design” consent frameworks and explanatory mechanisms sets the ethical trust of AI for health care cloud adoption AI for health care and clouds.

The jumble of data governance along with vendor relationnships make the United State’s situation more complex. Hospitals and healthcare systems rely on outside third parties Cloud Computing Service Provide Storage, Analytics and even Develop Algorithms, creating concentrated dependencies on mega corporations such as Google, Amazon and Microsoft (Rangel, 2021). This arrangement has shifted the control of sensitive patient data to vendors who, irrespective of contracts, care more about efficiency and scalability over patient-centric safeguards. The Project Nightingale case, where Google partnered with Ascension to gain access to millions of patient records, illustrates how weak contract terms and oversight can undermine public trust in healthcare institutions (Arigbabu et al., 2024). It has been noted that vendor contracts tend to neglect important aspects of data ownership, data provenance and permissible secondary uses, therefore, data governance becomes increasingly difficult to enforce (Salako et al., 2024). This results in the phenomenon of function creep, where the information collected from patients for the purpose of clinical care is utilized for research or even commercial development without the patient’s knowledge. Such secretive vendor contracts and relationships violate ethical principles of patient autonomy and trust, and even make regulatory oversight more difficult.

The rapid evolution which is technological progress is another major challenge, which is its impact on cloud-infrastructure architecture is used to consolidate massive fundamental areas of public health information, attracted the cloud to criminals (Bhardwaj, 2024). Unlike the on-premise, the breach of cloud systems, which is in the bridging phase, leads to a failure in the systems of communication of which multitude of patients is large severe in the operational as well as reputation aspects. Lack of know-how on to the cloud areas is a breach in security of cloud systems including a framework, configuration, standard enforced access, poor information trapping, and as well in advance identifying and minimizing the possibility of such vulnerabilities. In addition, multi-cloud access also fosters collaboration through partnerships which is In the United States, questions of accountability and liability still remain unanswered in the context of AI and healthcare systems. If an AI system hosted on the cloud provides detrimental recommendation, who is responsible? Clinicians may say they followed instructions given to them, while the hospitals may say the blame lies on the software developer who, in turn, blames the cloud operator hosting the infrastructure (Gerke, 2021). This diffusion of responsibility creates legal gray areas that current tort law and regulations surrounding medical devices, do not cover. Likewise, there are current devices that are in pertains to the proposed high-risk AI devices that, much to the scholars dismay, critics argue the AI systems are in place and functioning. There are also, however, pre-market and post-market controls that are available and tend atrial legal liability approach to the AI systems (Babalola et al., 2024). Though, under these systems, there is often inequitable distribution of the public interest and of the aforementioned systems and in turn, vendor capture (Babalola et al., 2024). Patients are not properly compensated for the damages they incur as a result of the lack of clear legal rules, while clinicians tend to avoid the subject of AI and focus on other domains, as there is a high legal exposure.

Lastly, weaknesses of the United States' current policies and legislation are enforcement and engaging the public. Singh (2023) states that although guidance and ethical principles have been provided by the federal bureaucracies, these are still "toothless" documents and lack the legal power to evoke state and institutional compliance. Some providers are heavily monitored, whilst others have a worrying lack of scrutiny. The problem of low public engagement persists. The very 'communities most impacted by the unfair systems' (Martinez-Martin et al, 2021) – e.g., racial and economic minorities – are most often, and most problematically, excluded from AI health cloud technologies development, deployment, and governance processes. Even where engagement takes place, it is often of a low quality 'consultation' type where the processes adopted do not genuinely affect the outcomes. The governance of these technologies, as a result, suffers from the lack of a social license to operate. The absence of adequate governance, alongside a lack of engagement from the oppressed communities, are the reasons why the United States will continue to face ethical and inequality issues (Williamson & Prybutok, 2024).

- *Opportunities of Navigating Ethics and Regulation in Artificial Intelligence Health Cloud in the US*

While challenging, the United States is also in a unique position to make use of the transformative potential of AI health cloud technologies to change the delivery of health care. One such opportunity is to improve clinical productivity (Babalola et al., 2024). AI cloud technology can improve the speed of diagnosis and treatment in disparate health systems by analyzing immense volumes of data nearly instantaneously (Zhang & Zhang, 2025). This is of immense value in US hospitals, which are already struggling with a shortage of medical personnel amid rising demands for management of chronic diseases (Adler-Milstein, 2023). AI-centric imaging systems can, for instance, cut the time to perform thousands of scans from hours to seconds, thereby, lightening the burden on radiologist and facilitating the timely delivery of patient care (Babalola et al., 2024). The cloud also allows even the smallest community hospitals to use advanced analytic tools without the exorbitant costs associated with on-site hardware. AI hosted in the cloud can, therefore, potentially provide access to advanced medical technologies to a wider patient population, as opposed to the traditional U.S. model which only provided them to a few selected highly prestigious institutions (Huang, 2024). If regulated properly, such technologies can widen access to healthcare to the underserved and, in doing so, alleviate the inequities in healthcare delivery.

AI health cloud also creates unique avenues for personalized medicine. AI cloud platforms allow the construction of models for individual risk assessment and treatment recommendations based on the aggregation of population-scaled genetic, lifestyle, and clinical datasets (Patel, 2023). Initiatives in the U.S. for precision medicine, such as the All of Us Research Program, utilize cloud architectures for the integration of large, diverse datasets from different patient populations. These architectures have the capacity to identify patients prone to developing conditions and intervene early, well before the onset of symptoms. Predictive models based on electronic health records, for example, are able to identify people with a high risk of developing clinical conditions such as sepsis or cardiovascular disease, reactive clinical measures can then be applied (Liu 2022). This capability fits the national policy objectives of the United States aimed at transitioning the health care system from managing diseases to the prevention of diseases. AI on the cloud, employed with the right strategy, can result in reduced expenses, better outcomes, and more patient-centered medicine.

Moreso, accessing and sharing data is another critical frontier. The U.S. healthcare system has faced the problem of siloed electronic health record (EHR) systems that undermine coordination across providers. AI health cloud platforms can divide these silos by constructing unified interoperable data ecosystems (Rosenbaum, 2021). This means that a cancer patient treated in one state can have their records electronically transferred to specialists in another, enhancing continuity of care. Cloud systems also enable large-scale collaborative clinical research, such as multi-site trials that aggregate data across multiple organizations (Babalola et al., 2024). This capacity to transcend institutional boundaries is beneficial for everyday clinical practice as well as advanced research. The US government's recent interoperability standards in the 21st Century Cures Act provide cloud platforms with a regulatory foundation to build on (Turner, 2023). Balancing the United States' technological capabilities with these legal frameworks will result in a more integrated and streamlined healthcare system.

The next sector of focus is the public health. AI health cloud has the potential to be transformative in this sector as well. For instance, in the cloud systems, health data at the population level is aggregated, enabling the cloud systems to monitor outbreaks of diseases in real time and respond to them as they happen. During the COVID crisis, cloud analytics was essential to the tethering of infections, modeling the capacity of hospitals, and the distribution of vaccines (Zhang, 2022). Other infrastructures can be used in the same manner to tackle chronic crises, such as the opioid crisis and diabetes, both of which require the analysis of large-scale data sets to formulate proper responses. Furthermore, the cloud infrastructures also allow the incorporation of unconventional public health data, such as of wearable devices and the social determinants of health (Babalola et al., 2024). This is crucial as the potential to integrate diverse sources of information, clinical and non-clinical data, has been identified as a way to begin systematically addressing health inequities in the United States (Evans, 2024). This is to say, the AI health cloud has the potential to be used as a clinical tool, and, in the hands of effective governance, she can also be a strategic public health planning resource.

Similarly, the growing access to new economic opportunities is noteworthy. Investment from both private and public players is driving innovation in the U.S. health AI cloud sector, which is among the fastest growing industries in the economy (Lichtenheim, 2024). Partnerships between cloud vendors and startups with hospitals are transforming diagnostics, drug discovery and operational management (Klein, 2023). AI in the cloud is now utilized in the pharmaceutical industry to model protein interaction and thus speed up drug development (Davis, 2023). U.S. is emerging as a global leader in digital health, with sustained innovation in AI cloud technology and advanced digital infrastructure. The cloud technology is also likely to cut the operational cost for hospitals by increasing the efficiency in administrative processes like billing and compliance, and reducing the physical infrastructure needed (Foster, 2022). The achieved savings can be utilized to provide better patient care, further increasing the long-term sustainability of the health system.

However, this requires sustained investment and focus, but, along with the overall resilience picture, cloud adoption also creates unique opportunities in cyber resilience. As technology improves, cloud systems does create new vulnerabilities, but, in any case, they employ far superior systems to manage risk than disaggregated on premise infrastructures (Lichtenheim, 2024). Many health care organizations, in any case, do not have the means to implement more enhanced threat deterrence solutions such as automated threat detection and real time threat monitoring, which leading vendors provide as part of the cloud (Baker, 2024). For instance, machine learning models deployed in the cloud can detect attempts at unauthorized data access before they morph into breaches of various scales. Already, federal industries have begun to work with, as part of the industry, to create proposed security frameworks to improve healthcare sector resilience and cyber systems (Agapito & Cannataro, 2023). If those frameworks take root, healthcare data may be more secure in the cloud than on premise systems. Hence, the almost universal notion of cloud computing as a weakness in cyber defense, if properly structured, offers an opportunity to improve the overall systems.

To innovate regulations and ethics; the U.S. is also in the unique position to lead. Although the system is still early in its development; there are an active group of scholars, advocacy organizations, and policymakers in the U.S. working on reforms to change the status quo (Gomase et al., 2025). Ideas on adaptive regulatory approaches, stronger audit frameworks, and ethics designed into practice, are increasingly being discussed and supported (Lewis, 2024). Pilot programs designed to implement ethical Thought Leadership (Sonani and Govindarajan, 2025) suggest these frameworks can be incorporated to cloud systems through mechanisms like continuous patient data oversight, fairness data audits, and consent dashboards. These developments show that ethics and regulations should no longer be considered to be trailing technology, but instead, can be advanced in relative harmony to transformational development. If the U.S. goes on to demonstrate investment in the further development of these governance frameworks; it shall be capable of setting boundaries on the behavior of the international community in the ethical use of AI health cloud systems. Beyond serving the interests of its people; this position would enable the U.S. to export its governance solutions to countries facing analogous issues.

Moreso, the US healthcare system stands to benefit from progress in cybersecurity. According to Bhardwaj (2024) and Salako et al. (2024), the industry is under constant assault from swarms of cybercriminals and needs secure robust cloud systems. Najana & Ranjan (2024) and Georgiou & Lambrinoudakis (2020) claim ‘security ‘by design’ is possible in cloud infrastructures through real-time threat processing, encryption, and automated compliance.’ For example, Sonani & Govindarajan (2025) and Du et al. (2024) show how reinforcement learning systems can be used to protect environments from tailored tactical cyber-attacks. Also, slack Bhardwaj (2024) recommends probes of cyber devices can furnish healthcare cloud ecosystems with proactive defenses. There is also the potential for AI secure cloud systems to enhance the geopolitical competitiveness of the US.

This dimension’s economy is underutilized. For example, IT in the Cloud reduces operational redundancy, reduces IT overheads, and enhances the performance of healthcare supply chains (Saratkar & Langote, 2024). Health systems can be Cloud-enabled by hospitals, and the resultant savings can be injected into clinical services (Singh, 2023). The AI health cloud, in addition, will accelerate the creation of whole new economies for the new vendors, businesses, and service providers. New titles like compliance auditors, AI ethicists, and cloud health consultants, for example, will be created with the further expansion of AI cloud services (Yandrapalli & Sharma, 2025). The US will strengthen its global leadership in the digital health economy, and its geopolitical influence, through the export of innovative health cloud technologies (Babalola et al., 2024).

Figure 2 shows an overview of the ground game-changing impact of AI health cloud technologies on healthcare governance and provision. It identifies six main points, such as Clinical Efficiency, which provides better triage and decision-making in faster diagnoses; Personalized Care, which involves customized treatments to specific patient data so that the results can be improved; Interoperability and Data Sharing, which insists on a seamless flow of the connection between the healthcare systems to ensure continuity of care and avoid data redundancy; Economic Growth and Innovation, which highlights the partnerships to provide technological improvements; and Cybersecurity Advancements, which focus on the necessity of strong threat detection to protect sensitive patient information. In sum, the figure summarizes why it is necessary to have integrated governance systems in place to make healthcare a safer, more efficient destination in the future.

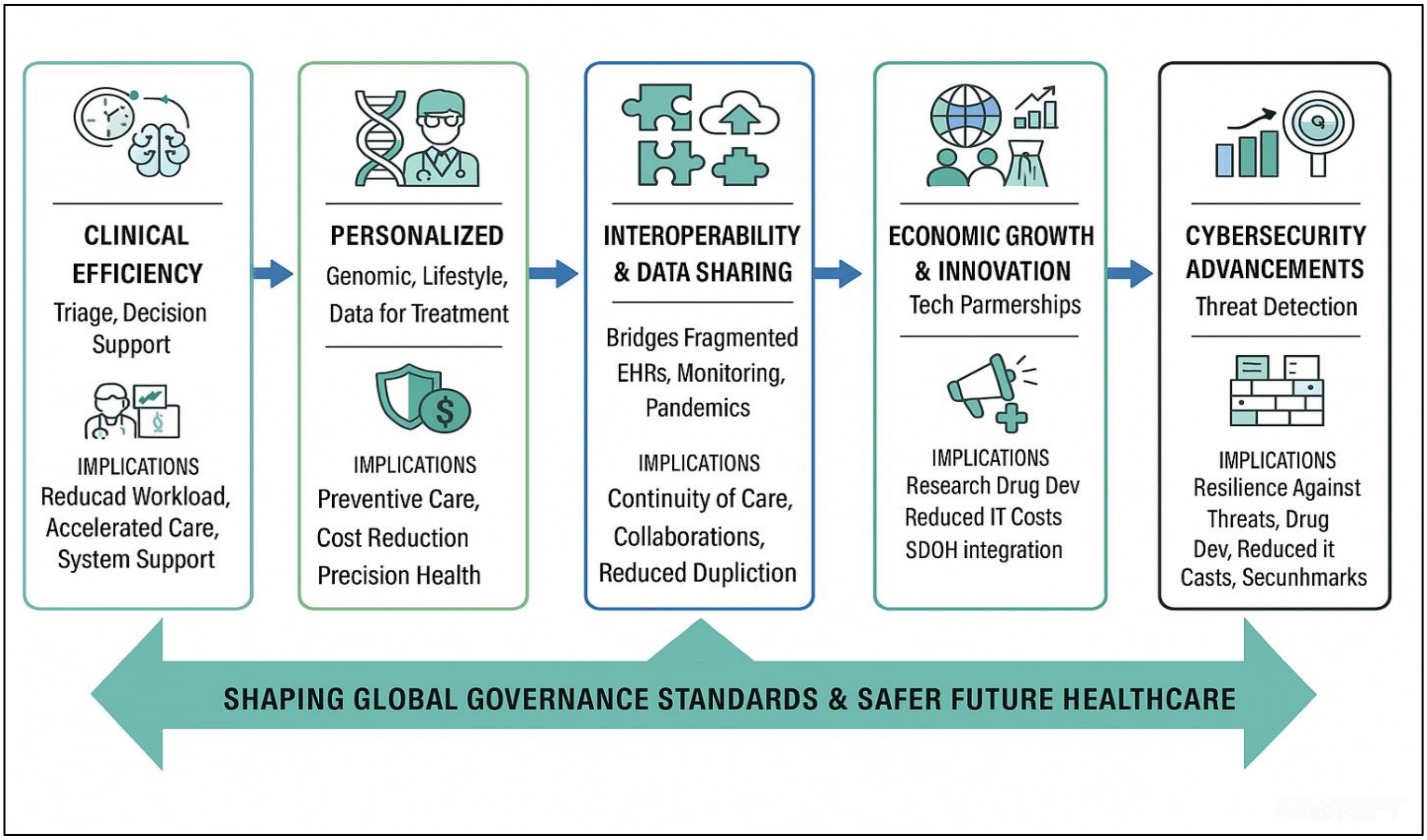
CLINICAL EFFICIENCY
Triage, Decision Support
IMPLICATIONS
Reducad Workload, Accelerated Care, System Support
PERSONALIZED
Genomic, Lifestyle, Data for Treatment
IMPLICATIONS
Preventive Care, Cost Reduction Precision Health
INTEROPERABILITY & DATA SHARING
Bridges Fragmented EHRs, Monitoring, Pandemics
IMPLICATIONS
Continuity of Care, Collaborations, Reduced Dupliction
ECONOMIC GROWTH & INNOVATION
Tech Parmerships
IMPLICATIONS
Research Drug Dev
Reduced IT Costs
SDOH integration
CYBERSECURITY ADVANCEMENTS
Threat Detection
IMPLICATIONS
Resilience Against Threats, Drug Dev, Reduced it Casts, Secunhmarks
SHAPING GLOBAL GOVERNANCE STANDARDS & SAFER FUTURE HEALTHCARE

Fig 2: Impact Areas of AI Health Cloud Technologies on Healthcare Governance
Source: Conceptual framework of the author based on the available research on AI, cloud computing, and regulation of healthcare.

III. CONCLUSION

Advancements in the U.S. artificial intelligence, cloud computing, and other technologies integrated within healthcare assist have greatly improved. Technology aids hospitals and other healthcare settings lighten the load of healthcare professionals, manage patient data and conduct research. Systems using AI and cloud technologies in healthcare boost the precision of real time chronic condition monitoring and diagnoses. Also, they enhance and optimize systems of healthcare and public healthcare services. This is one of the reasons U.S. healthcare services is perceived as cutting digital healthcare and digital healthcare systems as advancements and innovative. Nevertheless, other problems do remain. Examples include aata inequity, algorithm abuse, inequity and unregulated systems, trust deficit, algorithm bias, and inequity. Systems that incorporate clouds and other healthcare technologies monopolize healthcare and treatment facilities. Therefore, the complexity of unregulated systems regarding the use of AI and cloud technologies within healthcare systems demands responsible governance and the equitable use of AI and cloud systems as control systems.

Based on this, the design and development of AI health systems should not be an afterthought, but rather include ethics. Structures are required to safeguard patient rights, provide transparency in using data, and create social trust. The patient must be able to manage their personal health data and be assured that AI systems should be employed in a responsible way.

REFERENCES

[1]. Agapito, G., & Cannataro, M. (2023). An overview on the challenges and limitations using cloud computing in healthcare corporations. *Big Data and Cognitive Computing*, *7*(2), 68.

[2]. Ali, H., & Aysan, A. F. (2025). Ethical dimensions of generative AI: A cross-domain analysis using machine learning structural topic modeling. *International Journal of Ethics and Systems, 41*(1), 3–34.

[3]. Amugongo, L. M., Kriebitz, A., Boch, A., & Lütge, C. (2025). Operationalising AI ethics through the agile software development lifecycle: A case study of AI-enabled mobile health applications. *AI and Ethics*, *5*(1), 227–244.

[4]. Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data governance in AI-enabled healthcare systems: A case of the project Nightingale. *Asian Journal of Research in Computer Science, 17*(5), 85–107.

[5]. Babalola, O., Adedoyin, F. A., Ogundipe, F., Folorunso, A., & Nwatu, C. E. (2024). Policy framework for cloud computing: AI, governance, compliance and management. *Global Journal of Engineering and Technology Advances, 21*(2), 114–126.

[6]. Bhardwaj, A. (2024). *Cyber investigations of smart devices*. CRC Press.

[7]. Bouderhem, R. (2024). Shaping the future of AI in healthcare through ethics and governance. *Humanities and Social Sciences Communications, 11*(1), 1–12.

[8]. Du, H., Liu, M., Liu, N., Li, D., Li, W., & Xu, L. (2024). Scheduling of low-latency medical services in healthcare cloud with deep reinforcement learning. *Tsinghua Science and Technology*, *30*(1), 100–111.

[9]. Georgiou, D., & Lambrinoudakis, C. (2020, September). Cloud computing framework for e-health security requirements and security policy rules case study: A European cloud-based health system. In *International Conference on Trust and Privacy in Digital Business* (pp. 17–31). Springer International Publishing.

[10]. Gerke, S. (2021). Health AI for good rather than evil? The need for a new regulatory framework for AI-based medical devices. *Yale Journal of Health Policy, Law, and Ethics*, *20*, 432.

[11]. Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295–336). Academic Press.

[12]. Gomase, V. S., Ghatule, A. P., Sharma, R., Sardana, S., & Dhamane, S. P. (2025). Cloud computing facilitating data storage, collaboration, and analysis in global healthcare clinical trials. *Reviews on Recent Clinical Trials.*

[13]. Karimian, G., Petelos, E., & Evers, S. M. (2022). The ethical issues of the application of artificial intelligence in healthcare: A systematic scoping review. *AI and Ethics, 2*(4), 539–551.

[14]. Kokala, A. (2022). The intersection of explainable AI and ethical decision-making: Advancing trustworthy cloud-based data science models. *International Journal of All Research Education & Scientific Methods, 10*(12), 2166–2183.

[15]. Liaw, S. T., Liyanage, H., Kuziemsky, C., Terry, A. L., Schreiber, R., Jonnagaddala, J., & de Lusignan, S. (2020). Ethical use of electronic health record data and artificial intelligence: Recommendations of the primary care informatics working group of the international medical informatics association. *Yearbook of Medical Informatics, 29*(1), 51–57.

[16]. Lichtenheim, G. (2024). *Transforming e-governance with cloud-based AI: A systems methodology for implementation* (Doctoral dissertation, Stevens Institute of Technology).

[17]. Martinez-Martin, N., Luo, Z., Kaushal, A., Adeli, E., Haque, A., Kelly, S. S., ... & Milstein, A. (2021). Ethical issues in using ambient intelligence in healthcare settings. *The Lancet Digital Health, 3*(2), e115–e123.

[18]. Murphy, K., Di Ruggiero, E., Upshur, R., Willison, D. J., Malhotra, N., Cai, J. C., ... & Gibson, J. (2021). Artificial intelligence for good health: A scoping review of the ethics literature. *BMC Medical Ethics*, *22*(1), 14.

[19]. Najana, M., & Ranjan, P. (2024). Compliance and regulatory challenges in cloud computing: A sector-wise analysis. *International Journal of Global Innovations and Solutions*, *1*, 1–21.

[20]. Palaniappan, K., Lin, E. Y. T., & Vogel, S. (2024, February). Global regulatory frameworks for the use of artificial intelligence (AI) in the healthcare services sector. In *Healthcare* (Vol. 12, No. 5, p. 562). MDPI.

[21]. Prakash, S., Balaji, J. N., Joshi, A., & Surapaneni, K. M. (2022). Ethical conundrums in the application of artificial intelligence (AI) in healthcare—A scoping review of reviews. *Journal of Personalized Medicine*, *12*(11), 1914.

[22]. Prakash, S., Malaiyappan, J. N. A., Thirunavukkarasu, K., & Devan, M. (2024). Achieving regulatory compliance in cloud computing through ML. *Advanced International Journal of Multidisciplinary Research, 2*(2).

[23]. Rangel, M. A. (2021). *Military breaking boundaries: Implementing third-party cloud computing practices for data storage* (Doctoral dissertation, Walden University).

[24]. Rehan, H. (2023). AI-powered genomic analysis in the cloud: Enhancing precision medicine and ensuring data security in biomedical research. *Journal of Deep Learning in Genomic Data Analysis, 3*(1), 37–71.

[25]. Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. *Asian Journal of Research in Computer Science*, *17*(12), 66–88.

[26]. Saratkar, S., & Langote, M. (2024, October). Navigating the cloud: Enhancing healthcare through opportunities and challenges of cloud computing. In *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (pp. 1045–1050). IEEE.

[27]. Shah, V., & Konda, S. R. (2022). Cloud computing in healthcare: Opportunities, risks, and compliance. *Revista Española de Documentación Científica, 16*(3), 50–71.

[28]. Singh, K. (2023). Artificial intelligence & cloud in healthcare: Analyzing challenges and solutions within regulatory boundaries. *SSRG International Journal of Computer Science and Engineering, 10*(9), 1–9.

[29]. Sonani, R., & Govindarajan, V. (2025). Cloud integrated governance-driven reinforcement framework for ethical and legal compliance in AI-based regulatory enforcement. *Journal of Selected Topics in Academic Research, 1*(1).

[30]. Sun, L., Jiang, X., Ren, H., & Guo, Y. (2020). Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application. *IEEE Access, 8*, 101079–101092.

[31]. Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences, 14*(2), 675.

[32]. Yadav, N., Pandey, S., Gupta, A., Dudani, P., Gupta, S., & Rangarajan, K. (2023). Data privacy in healthcare: In the era of artificial intelligence. *Indian Dermatology Online Journal, 14*(6), 788–792.

[33]. Yandrapalli, V. K., & Sharma, S. (2025). Navigating the ethical and legal aspects of cloud-based systems. In *Cloud computing for smart education and collaborative learning* (p. 188).

[34]. Zhang, J., & Zhang, Z. M. (2023). Ethics and governance of trustworthy medical artificial intelligence. *BMC Medical Informatics and Decision Making, 23*(1), 7.