Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Balancing Innovation and Privacy: Addressing Surveillance Concerns in Healthcare AI Systems

Vittal Rao Baikadolla
Golden Gate University, San Francisco, USA
Corresponding Author: Vittal Rao Baikadolla **E-mail**: vittalrao@gmail.com

| ABSTRACT

Healthcare AI systems promise revolutionary advancements in opinion, treatment, and care delivery, yet produce unknown sequestration challenges as these technologies bear vast patient datasets to serve effectively. This pressure between invention and sequestration protection represents an abecedarian incongruity in healthcare's digital metamorphosis. Recent sequestration breaches, instigated by controversial data-participating hookups between healthcare systems and technology companies, have eroded public trust and stressed crunches in traditional concurrence models and nonsupervisory fabrics. The composition examines both specialized results, including allied literacy, discriminational sequestration, homomorphic encryption, and synthetic data generation, alongside governance fabrics emphasizing transparent concurrence mechanisms, specialized institutional review processes, multistakeholder involvement, and streamlined regulations. Addressing these challenges requires a balanced approach that preserves sequestration without stifling salutary invention, eventually maintaining the patient trust essential for healthcare advancement.

| KEYWORDS

Healthcare Privacy, Artificial Intelligence Ethics, Patient Consent, Federated Learning, Multistakeholder Governance.

| ARTICLE INFORMATION

ACCEPTED: 12 June 2025 **PUBLISHED:** 23 July 2025 **DOI:** 10.32996/jcsts.2025.7.7.101

1. Introduction

Patient care. The integration of AI systems across the healthcare spectrum has been expanding rapidly in recent times, encompassing operations in predictive analytics, medical imaging interpretation, substantiated drug recommendations, and functional effectiveness advancements. Machine learning algorithms have demonstrated remarkable capabilities in healthcare settings, with neural network infrastructures showing particular promise in individual settings across multiple medical specialties, including radiology, pathology, dermatology, and ophthalmology [1]. The eventuality of these technologies to compound clinical decision-making has attracted significant attention from healthcare providers, experimenters, policymakers, and business stakeholders worldwide.

This technological revolution presents an abecedarian sequestration incongruity that demands critical attention from the healthcare community. AI systems, particularly those grounded on deep learning infrastructures, bear vast amounts of patient data to develop accurate and dependable models. These systems thrive on large, different datasets that contain comprehensive patient information to identify patterns and induce perception. Yet healthcare operates within strict sequestration fabrics designed to cover patient confidentiality and autonomy. This creates an essential pressure that effective AI development depends on access to expansive medical records containing sensitive, particular information, while established ethical principles and legal regulations emphasize the protection of patient sequestration rights and informed consent [2]. The healthcare sector must navigate this complex geography while trying to realize the benefits of AI invention without compromising the core values of patient protection.

The sequestration challenges associated with healthcare AI've formerly manifested in several high-profile difficulties that illuminate the difficulties in balancing technological advancement with sequestration safeguards. A notable illustration involves the collaboration between a major public healthcare system and a prominent technology company for the development of a mobile operation concentrated on acute order injury discovery and operation. This cooperation involved the transfer of patient data without carrying specific consent for AI development, pressing critical gaps in governance fabrics girding healthcare AI executions [2]. The incident raised significant concerns about data privacy practices and the acceptability of being nonsupervisory mechanisms to address the unique challenges posed by AI technologies in healthcare settings.

Similar cases illustrate broader enterprises about surveillance capabilities embedded within healthcare AI systems. As these technologies collect, dissect, and use increasingly granular patient information, they produce unknown visibility into individuals' most intimate health details. This surveillance implicit extends beyond traditional healthcare boundaries when data is shared with technology companies whose business models may involve data application beyond the immediate healthcare operation. The threat of function creep, where data collected for one specific healthcare purpose gradually becomes habituated for fresh, potentially unauthorized purposes, represents a significant concern for cases and sequestration lawyers alike [2]. The expansion of data collection, analysis, and participation capabilities eased by AI raises abecedarian questions about applicable boundaries and safeguards in healthcare information operations.

The effective integration of AI in healthcare thus requires robust sequestration- conserving fabrics that maintain public trust while enabling invention. This delicate balance necessitates both specialized results that cover data integrity and confidentiality, and governance structures that ensure transparency, responsibility, and patient autonomy. The governance of health information in the AI environment involves complex considerations around concurrence models, data power, algorithmic translucency, and responsibility mechanisms [1]. As healthcare systems worldwide increasingly embrace AI capabilities, addressing these sequestration and surveillance enterprises becomes essential not only for ethical practice but also for sustaining the patient trust upon which healthcare unnaturally depends. The ensuing sections examine these challenges in depth and propose comprehensive approaches to resolve the pressure between AI advancement and sequestration protection in healthcare settings.

2. The Data Dilemma in Healthcare AI

The development of effective healthcare AI systems unnaturally depends on access to massive, diverse clinical datasets. Contemporary machine learning approaches, particularly deep neural networks, require substantial training data to achieve performance levels respectable for clinical application. Healthcare data exists in complex, miscellaneous formats, including structured electronic health records, unstructured clinical notes, high-resolution medical images, genomic sequences, and nonstop monitoring data from medical bias. The complexity and volume of this information present significant computational and organizational challenges. Exploration indicates that data preparation and drawing generally consumes roughly 80% of AI development time in healthcare settings, with substantial coffers devoted to harmonizing inconsistent data formats, addressing missing values, and correcting incorrect entries. Healthcare institutions face significant structure walls when trying to aggregate sufficient data for AI development, including heritage systems with limited interoperability, departmental data silos, and inconsistent attestation practices. These specialized challenges are compounded by organizational walls such as contending institutional precedents, limited specialized moxie, and enterprises about competitive advantages. A governance frame for healthcare AI must thus address not only sequestration protections but also the licit need for data access to develop clinically useful systems [3].

Healthcare data occupies a uniquely sensitive position among particular information orders due to its intimate nature and eventuality for demarcation or stigmatization if misused. Medical records contain comprehensive details about physical and internal health conditions, inheritable tendencies, reproductive history, substance use, and other deeply particular aspects of mortal experience. The perceptivity of this information is honored in technical healthcare sequestration regulations worldwide. Ultramodern healthcare data increasingly incorporates information from sources beyond traditional clinical surroundings, including consumer wearable bias, social media exertion, coping actions, and environmental exposures. This expanding description of applicable health information creates new sequestration challenges as the boundaries between clinical and consumer data blur. Healthcare data breaches have increased significantly in recent times, with substantial fiscal and reputational consequences for affected institutions and cerebral torture for cases whose information is compromised. The specialized characteristics of machine literacy systems produce fresh sequestration vulnerabilities, as these systems may inadvertently study rare or unique patient information during training, potentially exposing this sensitive data through model labor. Sequestration enterprises are further amplified when considering algorithmic impulses that might disproportionately affect vulnerable populations, creating implicit demarcation pitfalls beyond direct sequestration violations [3].

The nonsupervisory geography governing healthcare data operations in AI development reflects evolving attempts to balance invention with protection. Established healthcare sequestration fabrics such as HIPAA, in the United States, were designed primarily for traditional data processing rather than the iterative, opaque nature of machine learning systems. These regulations generally rely on generalities such as de-identification and informed consent that present perpetration challenges in the AI environment. The effectiveness of traditional de-identification methods has been questioned as machine learning styles demonstrate adding capability to re-identify anonymous data through pattern recognition across multiple datasets. Conventional informed consent models face significant limitations when applied to AI development, as the implicit future uses of data in algorithmic systems may not be completely known at the time of collection. Newer regulations similar to GDPR incorporate provisions more directly applicable to algorithmic systems, including conditions for data minimization, purpose limitation, and rights to explanation for automated opinions. These nonsupervisory fabrics produce complex compliance conditions for healthcare AI inventors, particularly those operating across multiple authorities with inconsistent norms. The fleetly evolving nature of AI technology frequently outpaces nonsupervisory adaptation, creating queries regarding compliance conditions for new operations [4].

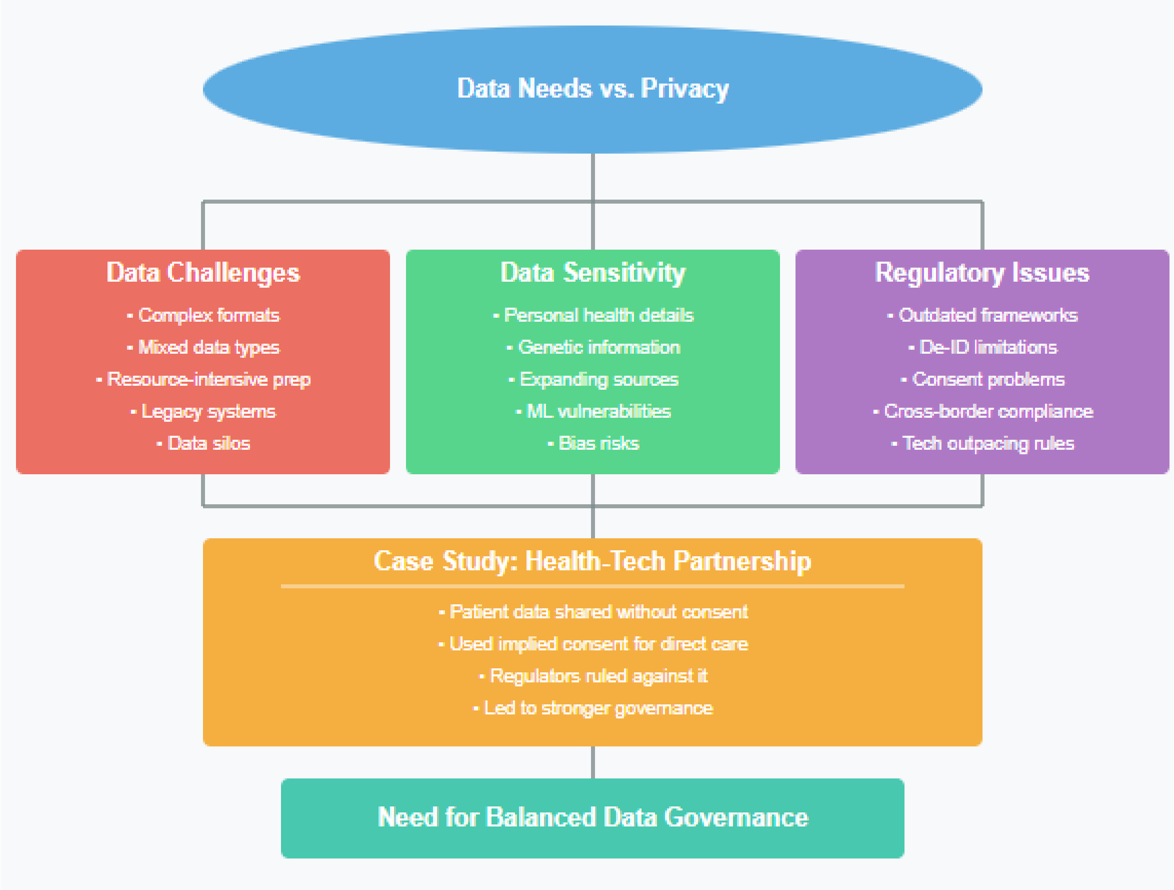

Fig 1: The Data Dilemma in Healthcare AI [3, 4]

A prominent case study illustrating these challenges involves the collaboration between a public health system and a leading technology company for developing a mobile operation to detect acute order injury. This cooperation, initiated as a data sharing agreement, exemplifies the complex interplay between invention pretensions and sequestration protections in healthcare AI development. The arrangement involved transferring case records containing detailed clinical information without carrying specific concurrence for this purpose, operating rather under inferred concurrence vittles for direct care conditioning. A disquisition by the public data protection authority concluded that cases would not willingly share their information to be used by a marketable technology inventor under the guise of vittles, for implicit clinical benefits. The ruling emphasized several critical governance failures, including shy translucency regarding data operation, inadequate consideration of lower sequestration-invasive druthers, and unhappy emulsion of exploration and clinical care conditioning. This case demonstrates how, indeed, technically sophisticated associations with significant coffers may fail to adequately address the unique sequestration and governance conditions of healthcare AI development. The contestation redounded in strengthened data governance conditions, including expanded translucency scores, clearer limitations on marketable operation of public healthcare data, and more robust oversight mechanisms for data participating arrangements. These issues illustrate the evolving norms for responsible data stewardship in healthcare AI development, particularly regarding the part of patient consent, marketable involvement, and nonsupervisory oversight [4].

3. Privacy Breaches and Public Trust

Data breaches and abuse in healthcare settings have unnaturally altered the geography of patient trust in medical institutions. The healthcare sector has become a primary target for data breaches, with incidents increasing dramatically in recent times. These breaches extend beyond simple unauthorized access to include ransomware attacks, bigwig pitfalls, and indecorous data handling practices. The consequences extend far beyond immediate fiscal penalties, creating continuing damage to the provider-patient relationship that forms the foundation of effective healthcare delivery. Research examining patient stations following publicized data incidents reveals significant behavioral changes, including increased withholding of sensitive information during clinical hassles, disinclination to share electronic health records with specialists, and dropped participation in health information exchanges. This corrosion of trust creates a paradoxical situation where sequestration enterprises lead cases to withhold information that might be pivotal for applicable care, potentially compromising clinical issues. The issue becomes particularly acute in the environment of artificial intelligence operations, where comprehensive data collection is essential for system performance. Healthcare institutions must now navigate a complex trust geography where sequestration protections serve as both a legal demand and a prerequisite for maintaining patient confidence. Institutions with robust sequestration fabrics and transparent data practices demonstrate measurably advanced situations of patient trust, suggesting that sequestration protection should be viewed not as a handicap to invention but as an enabler of responsible data application [5].

Traditional concurrence models have proven shy for addressing the complex sequestration counteraccusations of healthcare AI operations. The informed consent paradigm, developed primarily for separate clinical interventions or exploration studies, assumes that cases can be given specific information about how their data will be used. This model faces abecedarian challenges when applied to machine literacy systems that continuously evolve and may be applied to purposes not anticipated during original data collection. Broad consent approaches, which seek patient authorization for unidentified unborn uses, raise questions about whether similar consent can be considered truly informed when the implicit operations remain undetermined. The specialized complexity of AI systems creates fresh walls to meaningful concurrence, as most cases warrant the technical knowledge demanded to understand how these systems reuse their particular information. This complexity extends to healthcare providers, who may be responsible for carrying out concurrence without completely understanding the technologies involved. Research examining cases' appreciation of AI-related concurrence documents indicates methodological gaps in understanding, particularly regarding secondary data uses, algorithmic decision-making processes, and implicit sequestration pitfalls. These challenges are amplified for vulnerable populations, including those with limited health knowledge, language barriers, or cognitive impairments. The concurrence riddle highlights the need for indispensable governance approaches that distribute responsibility beyond individual cases to include institutional responsibility mechanisms, ethical oversight, and nonsupervisory fabrics specifically designed for healthcare AI operations [6].

Secondary uses of healthcare data represent a growing area of concern within the healthcare AI ecosystem. Data originally collected for direct case care is increasingly repurposed for algorithm development, quality enhancement, marketable product development, and exploration operations. Healthcare institutions frequently navigate complex ethical and legal terrain when determining applicable secondary uses, particularly when marketable realities are involved in data processing. While cases generally express support for using their health information to advance medical knowledge and ameliorate care for others, this amenability decreases significantly when marketable profit enters the equation. The perception that private parties may profit financially from patient data without corresponding compensation to data subjects raises questions of fairness and exploitation. Healthcare associations face mounting pressure to develop transparent data governance frameworks that easily communicate how patient information may be used beyond direct care purposes. These fabrics must address not only traditional sequestration considerations but also emerging concerns about algorithmic bias, data power, and the unequal distribution of benefits derived from collaborative health information. Healthcare institutions increasingly recognize that maintaining patient trust requires going beyond minimal legal compliance to address broader ethical considerations regarding secondary data use, particularly as the boundaries between clinical care, quality enhancement, and marketable development come increasingly blurred in the healthcare AI geography [5].

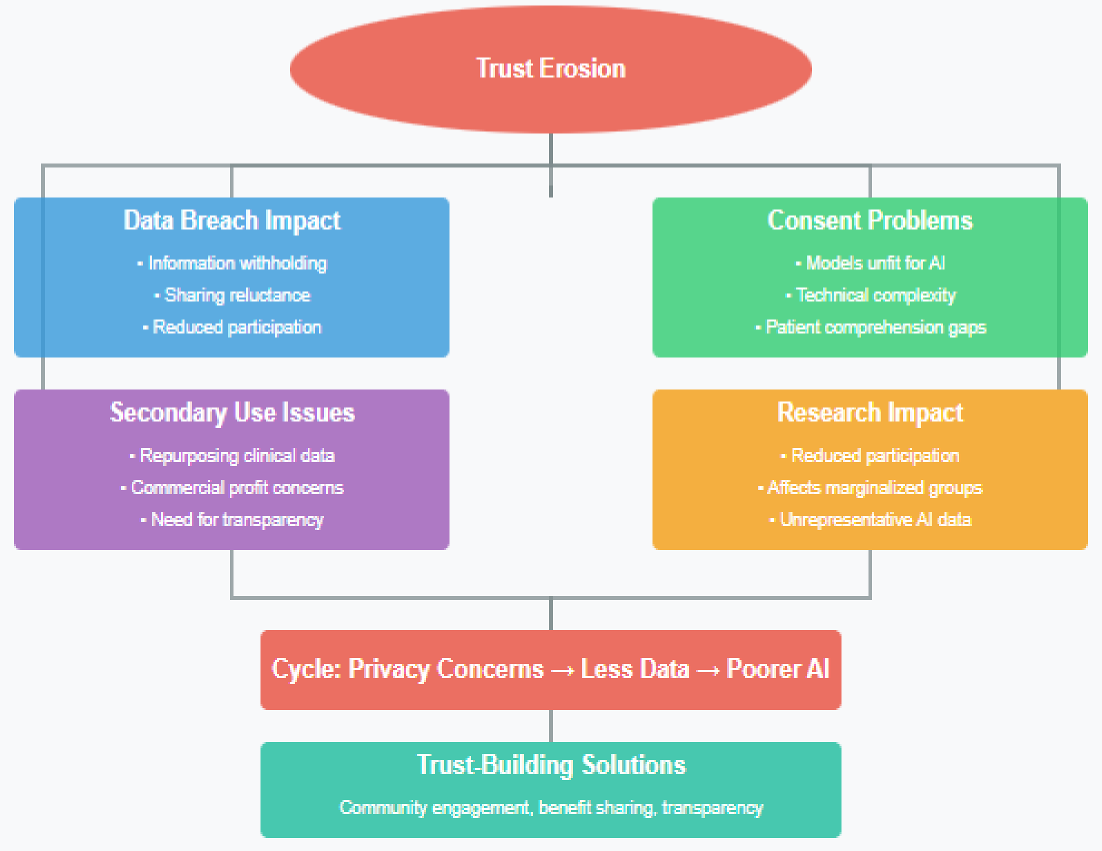
Trust Erosion
Data Breach Impact
• Information withholding
• Sharing reluctance
• Reduced participation
Consent Problems
• Models unfit for AI
• Technical complexity
• Patient comprehension gaps
Secondary Use Issues
• Repurposing clinical data
• Commercial profit concerns
• Need for transparency
Research Impact
• Reduced participation
• Affects marginalized groups
• Unrepresentative AI data
Cycle: Privacy Concerns → Less Data → Poorer AI
Trust-Building Solutions
Community engagement, benefit sharing, transparency

Fig 2: Privacy Breaches and Public Trust [5, 6]

The corrosion of trust stemming from sequestration enterprises threatens to undermine participation in licit medical exploration, potentially creating significant barriers to medical advancement. Public stations toward health data participation live on a spectrum determined by multitudinous factors, including perceived benefit, institutional character, data perceptivity, and individual sequestration enterprises. Declining trust in healthcare institutions represents a significant hedge to exploration participation, with counteraccusations for both the volume and representativeness of available data. This trust deficiency appears particularly pronounced among populations that have historically experienced discrimination or mistreatment in healthcare settings, including ethnical minorities and socioeconomically underprivileged groups. The performing participation difference hinders immortalizing or complicating being healthy injuries by creating exploration datasets that do not deficiently represent different populations. Algorithms trained on these unrepresentative datasets may perform inadequately when applied to underrepresented groups, creating a cyclical problem where sequestration enterprises lead to rejection, which in turn leads to technologies that serve these populations less effectively. Healthcare experimenters increasingly fete the need to proactively address trust deficits through community engagement, benefit-participating arrangements, and transparent data stewardship practices. Successful approaches emphasize cooperation rather than competition, with affected communities having meaningful input into exploration precedents and data governance. Healthcare institutions must navigate the complex interaction between sequestration protection, trust structure, and indifferent representation in exploration, factoring that these factors inclusively determine the social license for data-intensive healthcare invention [6].

4. Technical Solutions for Privacy-Preserving AI

Federated literacy enables a cooperative model training without polarizing sensitive case data, addressing an abecedarian challenge in healthcare AI development. This approach trains algorithms across multiple decentralized biases or waiters holding original data samples, swapping only model updates rather than raw data. Federated literacy has particular applicability in healthcare where data silos live across institutions due to nonsupervisory constraints and competitive enterprises. Executions gauge colorful operations including medical imaging analysis, clinical decision support, and predictive analytics. While offering significant sequestration advantages, several specialized challenges remain, including communication effectiveness across networks with varying bandwidth, computational diversity among sharing institutions, and statistical diversity of patient populations across spots. Despite these sequestration advantages, allied literacy isn't vulnerable to implicit vulnerabilities, including class inference, model inversion, and property conclusion attacks. The fashion can be enhanced through reciprocal styles including discriminational sequestration, secure aggregation protocols, and robustness against inimical actors [7].

Differential sequestration provides a fine frame for quantifying and limiting sequestration pitfalls through precisely calibrated statistical noise. This approach offers formal guarantees against re-identification regardless of an adversary's background knowledge or computational power. The abecedarian principle ensures that including or banning any single case's information has a rigorously limited effect on analysis issues, creating presumptive deniability for all individualities. Perpetration approaches include the Laplace medium, the Gaussian medium, and the exponential medium. Healthcare operations present unique challenges due to data complexity and perceptivity. The high dimensionality of healthcare information increases the sensitivity of calculations, making larger noise additions that may compromise accuracy. Longitudinal healthcare data presents fresh complications, as repeated compliances of the same case can quickly exhaust sequestration budgets. Differential sequestration has been successfully applied across colorful disciplines, including clinical trial data sharing, complaint surveillance, genomic studies, and machine learning model training [8].

Homomorphic encryption and secure multi-party calculation enable calculation on encrypted data without exposing sensitive information. Homomorphic encryption allows operations to be performed directly on translated data, producing translated results that, when deciphered, match results from operations on unencrypted data. Different variants offer different capabilities. Incompletely homomorphic encryption supports limited operations, while completely homomorphic encryption supports arbitrary calculations but with significant computational overhead. Secure multi-party calculation allows multiple parties to concertedly cipher functions over combined data while keeping individual inputs private, using methods including secret sharing, garbled circuits, and oblivious transfer [7].

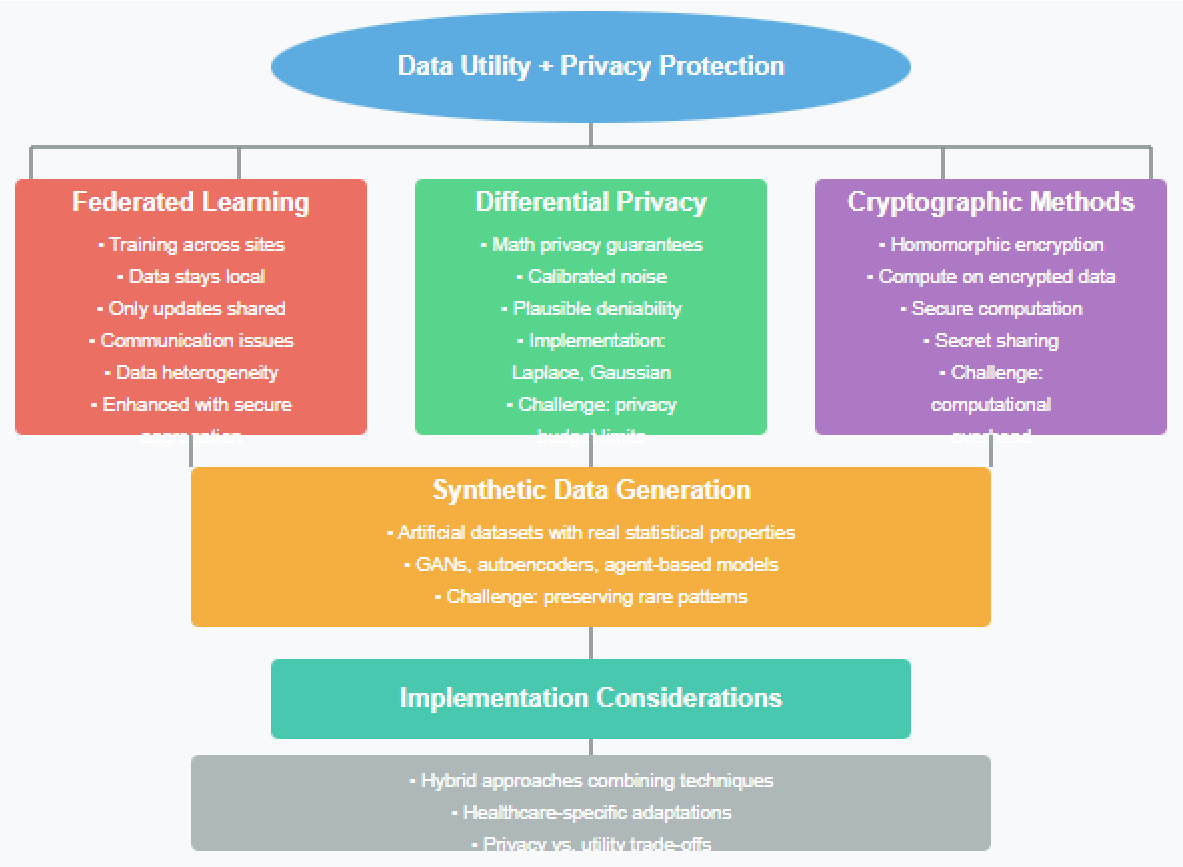
Data Utility + Privacy Protection
Federated Learning
• Training across sites
• Data stays local
• Only updates shared
• Communication issues
• Data heterogeneity
• Enhanced with secure aggregation
Differential Privacy
• Math privacy guarantees
• Calibrated noise
• Plausible deniability
• Implementation: Laplace, Gaussian
• Challenge: privacy budget limits
Cryptographic Methods
• Homomorphic encryption
• Compute on encrypted data
• Secure computation
• Secret sharing
• Challenge: computational overhead
Synthetic Data Generation
• Artificial datasets with real statistical properties
• GANs, autoencoders, agent-based models
• Challenge: preserving rare patterns
Implementation Considerations
• Hybrid approaches combining techniques
• Healthcare-specific adaptations
• Privacy vs. utility trade-offs

Fig 3: Technical Solutions for Privacy-Preserving AI [7, 8]

Sequestration- conserving synthetic data generation creates artificial datasets, maintaining statistical parcels of real case data without exposing factual records. Methodological approaches include generative adversarial networks, variational autoencoders, and agent-grounded simulation models. Perpetration involves preprocessing real data, training a generative model, generating synthetic records, and validating both mileage and sequestration. Healthcare data presents unique challenges due to complex temporal connections, rare but significant events, and intricate correlations across multiple modalities. Synthetic data facilitates exploration, collaboration across institutional boundaries, external confirmation of findings, algorithm development, and software testing without exposing real patient information [8].

5. Policy and Governance Frameworks

Transparent concurrence mechanisms designed specifically for AI operations represent a critical elaboration beyond traditional healthcare concurrence models. Standard informed consent protocols were developed for separate medical interventions or conventional exploration studies, surroundings that differ mainly from the nonstop, evolving nature of AI systems. These differences include algorithmic nebulosity, eventuality for unexpected operations, complex data processing chains, and probabilistic labor. Research examining case appreciation of standard concurrence forms when applied to AI operations reveals significant gaps in understanding regarding data relation, eventuality for re-identification, algorithmic bias, and unborn secondary uses. Proposed advancements include layered concurrence approaches presenting information in progressive situations of detail, dynamic concurrence fabrics enabling cases to modify warrants over time, and multimedia platforms incorporating visual explanations and interactive rudiments. Perpetration walls include developing scalable systems, addressing varying situations of technological knowledge, and determining applicable norms for retrospective analysis of big datasets [9].

Institutional review processes for AI-grounded data-participating enterprises bear substantial elaboration beyond traditional exploration ethics frameworks. Conventional institutional review boards face limitations when assessing AI systems due to review processes designed for traditional clinical studies, inadequate specialized moxie among pundits, difficulties assessing implicit algorithmic damages, and challenges determining applicable oversight boundaries between quality enhancement and formal exploration. Technical AI ethics panels have surfaced as a reciprocal approach, incorporating interdisciplinary moxie, gauging clinical drug, computer wisdom, ethics, law, and patient advocacy. These panels employ structured assessment frameworks examining data provenance, algorithmic translucency, fairness evaluation, sequestration protection measures, and benefit-threat assessments. Evaluation methodologies have evolved toward nonstop monitoring throughout the AI lifecycle, with an emphasis on post-deployment surveillance. Threat-stratified review pathways have surfaced, with low-threat operations entering expedited assessment while high-threat operations suffer comprehensive review [10].

Effective healthcare AI governance requires meaningful involvement from different stakeholders throughout development and deployment. Multistakeholder models incorporate perspectives from healthcare providers, cases, specialized inventors, executive leaders, nonsupervisory experts, and ethics specialists. Case involvement has evolved from tokenistic representation toward meaningful participation through premonitory boards, governance commission representation, and methodical feedback objectification. Methodologies include deliberative forums exploring value dicker, participatory design sessions, and community discussions regarding respectful data uses. Healthcare provider involvement ensures systems align with clinical workflows and professional values. Translucency mechanisms represent critical governance factors, with public-facing attestation, clear exposure of data operation, and accessible explanations of algorithmic processes [9].

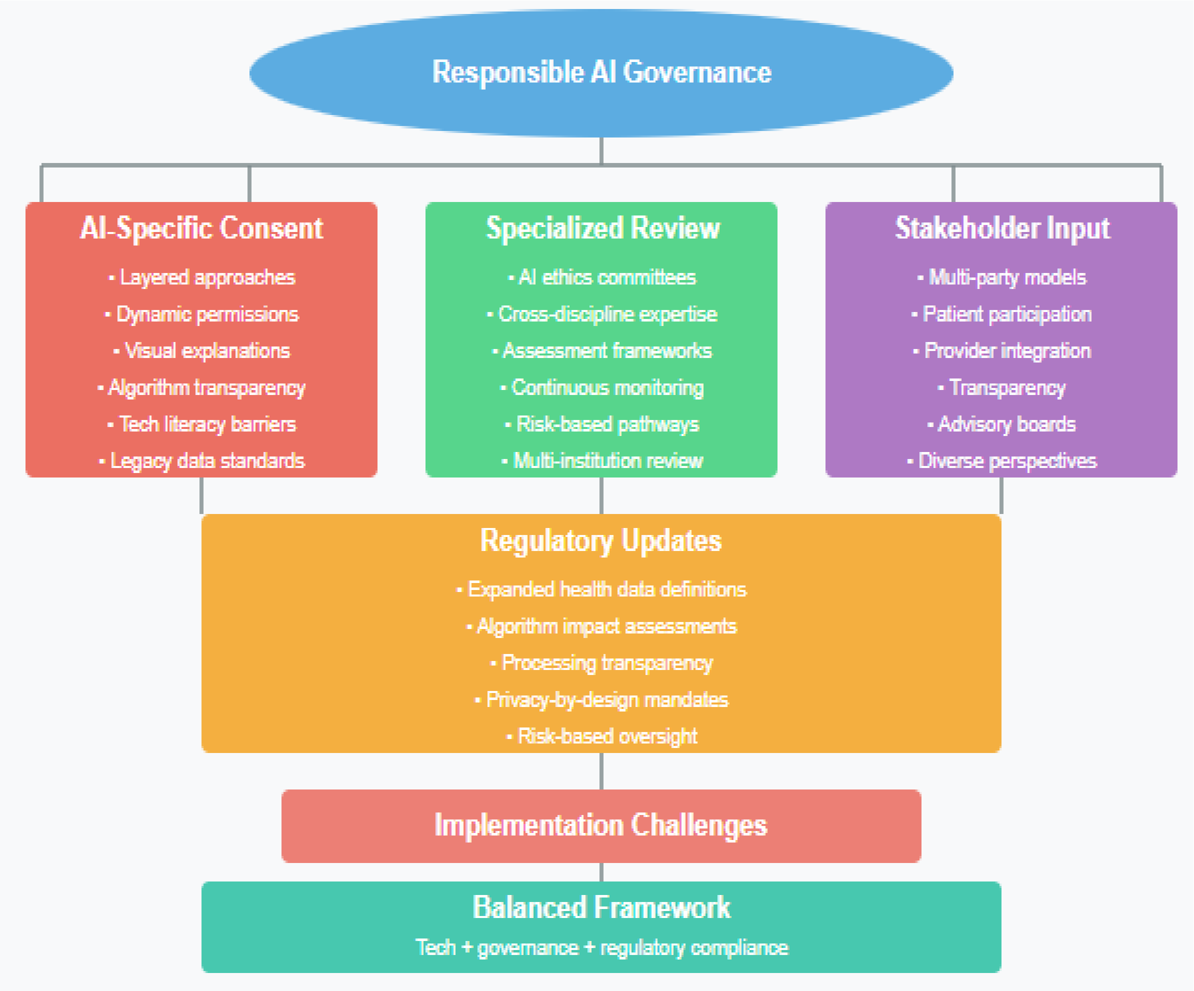

Fig 4: Policy and Governance Frameworks [9, 10]

Regulatory frameworks governing healthcare AI sequestration bear significant streamlining to address arising challenges. Current regulations contain substantial gaps regarding algorithmic processing, creating queries for inventors and cases. Generalities similar to identifiability, concurrence, data minimization, and purpose specification present perpetration challenges in complex machine learning environments. Emerging nonsupervisory models have begun addressing these gaps through detailed delineations of defended information, algorithmic impact assessment conditions, translucency scores, and obligatory sequestration-by-design principles. Threat-grounded fabrics show pledge, with commensurate oversight applied to implicit sequestration pitfalls. Perpetration challenges include balancing invention with protection, addressing rapid-fire technological elaboration, and developing specialized compliance norms [10].

6. Conclusion

The integration of AI into healthcare demands thoughtful navigation of the pressure between technological advancement and sequestration protection. Success depends on developing reciprocal strategies across multiple disciplines, enforcing sequestration- conserving specialized infrastructures, redesigning concurrence processes for algorithmic surrounds, establishing technical governance bodies with different moxie, and streamlining nonsupervisory fabrics to address arising challenges. Sequestration protection should be reconceptualized not as a handicap to invention but as an abecedarian enabler that maintains the trust necessary for cases to share information powering AI systems. Organizations that proactively address sequestration enterprises through both specialized safeguards and robust governance will gain competitive advantages through enhanced case trust and data access. Moving forward, healthcare institutions must commit to responsible data stewardship that balances invention imperatives with ethical considerations to cover patient sequestration, ensuring that maintaining public confidence remains essential to realizing the transformative eventuality of AI in healthcare.

Funding: This research received no external funding

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

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

References

[1] Alvin R et al., (2019) Ensuring Fairness in Machine Learning to Advance Health Equity, National Library of Medicine, 2019. https://pmc.ncbi.nlm.nih.gov/articles/PMC6594166/

[2] Blake M, (2021) Privacy and artificial intelligence: challenges for protecting health information in a new era, BMC Medical Ethics, 2021. https://link.springer.com/content/pdf/10.1186/s12910-021-00687-3.pdf

[3] Cynthia D and Aaron R, (2014) The Algorithmic Foundations of Differential Privacy, NOW, 2014. https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf

[4] Ezekiel J. and Emanuel et al., (2006) What Makes Clinical Research Ethical? JAMA, 2006. https://www.dartmouth.edu/cphs/docs/jama-article.pdf

[5] Julia P and Hal H, (2017) Google DeepMind and healthcare in an age of algorithms, Springer, 2017. https://link.springer.com/article/10.1007/s12553-017-0179-1

[6] Nicholson P W. II and Glenn C I., (2019) Privacy in the Age of Medical Big Data, University of Michigan, 2019. https://repository.law.umich.edu/articles/2764/

[7] Peter K et al., (2021) Advances and Open Problems in Federated Learning, arXiv:1912.04977, 2021. https://arxiv.org/abs/1912.04977

[8] Priyank J et al., (2016) Big data privacy: a technological perspective and review, ResearchGate, 2016. https://www.researchgate.net/publication/310898657_Big_data_privacy_a_technological_perspective_and_review

[9] Sandeep R et al., (2019) A governance model for the application of AI in healthcare, *Journal of the American Medical Informatics Association*, 2019. https://pmc.ncbi.nlm.nih.gov/articles/PMC7647243/pdf/ocz192.pdf

[10] Thomas D and Ravi K, (2019) The potential for artificial intelligence in healthcare, National Library of Medicine, 2019. https://pmc.ncbi.nlm.nih.gov/articles/PMC6616181/