p-ISSN: 2708-2474
e-ISSN: 2708-2482

www.gmsrjournal.com
GMSR
Global Management Sciences Review
managing humanity

GMSR

GLOBAL MANAGEMENT SCIENCES REVIEW

HEC-RECOGNIZED CATEGORY-Y

VOL. X, ISSUE III, SUMMER (SEPTEMBER-2025)

DOI (Journal): 10.31703/gmsr
DOI (Volume): 10.31703/gmsr.2025(X)
DOI (Issue): 10.31703/gmsr.2025(X-III)

Double-blind Peer-review Research Journal
www.gsrjournal.com

HumanityPublications
sharing research

Humanity Publications (HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Article title

Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning

Abstract

With the spread of Machine Learning (ML) and Artificial Intelligence (AI) in the healthcare sector, the regulatory structures that currently dominate the field (particularly HIPAA law in the United States) have become unable to deal with emerging challenges and opportunities offered by health data utilization. This paper argues that the growing trend of predictive analytics and algorithmic evaluations needs governance models that go beyond the standard perimeter-centric and consent-based paradigm of HIPAA. By identifying key governance issues, such as algorithmic bias, data provenance, dynamic consent, federated learning architectures, and power asymmetries in the data ecosystems, the article suggests a multi-layered governance model, which should be based on the principles of accountability, fairness, transparency, data stewardship, and multi-stakeholder co-regulation. Along with the application of this model in clinical diagnostics, public health research, and business analytics, periodic reassessment of health data regulations is highly emphasized to protect health data privacy.

Keywords: Health Data Governance; Machine Learning; Hipaa Reform; Algorithmic Accountability; Data Stewardship; Privacy-Sensitive AI.

Authors:

Ahmed Raza: (Corresponding Author)
LLM Scholar, Pennsylvania State University, USA.
Email: (ahmedraza.sajjad@gmail.com)

Shahzad Khalid: Doctoral Researcher, Brunel University London, United Kingdom.
Assistant Professor, Department of Law, Superior University, Lahore, Punjab, Pakistan.

Ali Nawaz Khan: Assistant Professor,. University Law College, University of the Punjab, Lahore, Punjab, Pakistan.

Pages: 114-123
DOI:10.31703/gssr.2025(X-III).11
DOI link: https://dx.doi.org/10.31703/gmsr.2025(X-III).11
Article link: http://www.gmsrjournal.com/articlebeyond-hipaa-rethinking-health-data-governance-in-the-age-of-machine-learning
Full-text Link: https://gmsrjournal.com/articlebeyond-hipaa-rethinking-health-data-governance-in-the-age-of-machine-learning
Pdf link: https://www.gmsrjournal.com/jadmin/Auther/31rvIolA2.pdf

Global Management Science Review

p-ISSN: 2708-2474 e-ISSN: 2708-2482
DOI(journal): 10.31703/gmsr
Volume: X (2025)
DOI (volume): 10.31703/gmsr 2025(X)
Issue: III (Spring-September 2025)
DOI(Issue): 10.31703/gmsr.2025(X-III)

Home Page
www.gmsrjournal.com

Volume: X (2025)
https://www.gmsrjournal.com/Current-issues

Issue: III-Summer (September-2025)
https://www.gmsrjournal.com/issue/9/3/2025

Scope
https://www.gmsrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gmsr/submissions

Google Scholar

Visit Us

Humanity Publications (HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Citing Article

11	Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning		
Authors	Ahmed Raza Shahzad Khalid Ali Nawaz Khan	DOI	10.31703/gmsr.2025(X-III).11
		Pages	114-123
		Year	2025
		Volume	X
		Issue	III

Referencing & Citing Styles

APA	Raza, A., Khalid, S., & Khan, A. N. (2025). Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning. *Global Management Sciences Review*, *X*(III), 23-28. https://doi.org/10.31703/gmsr.2025(X-III).11
CHICAGO	Raza, Ahmed, Shahzad Khalid, and Ali Nawaz Khan. 2025. "Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning." *Global Management Sciences Review* X (III):23-28. doi: 10.31703/gmsr.2025(X-III).11.
HARVARD	RAZA, A., KHALID, S. & KHAN, A. N. 2025. Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning. *Global Management Sciences Review,* X**,** 23-28.
MHRA	Raza, Ahmed, Shahzad Khalid, and Ali Nawaz Khan. 2025. 'Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning', *Global Management Sciences Review*, X: 23-28.
MLA	Raza, Ahmed, Shahzad Khalid, and Ali Nawaz Khan. "Beyond Hipaa: Rethinking Health Data Governance in the Age of Machine Learning." *Global Management Sciences Review* X.III (2025): 23-28. Print.
OXFORD	Raza, Ahmed, Khalid, Shahzad, and Khan, Ali Nawaz (2025), 'Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning', *Global Management Sciences Review,* X (III), 23-28.
TURABIAN	Raza, Ahmed, Shahzad Khalid, and Ali Nawaz Khan. "Beyond Hipaa: Rethinking Health Data Governance in the Age of Machine Learning." *Global Management Sciences Review* X, no. III (2025): 23-28. https://dx.doi.org/10.31703/gmsr.2025(X-III).11.

e-ISSN: 2708-2482 Volume: X (2025) Issue: III-Summer (September-2025) p-ISSN: 2708-2474

Global Management Sciences Review
www.gmsrjournal.com
DOI: http://dx.doi.org/10.31703/gmsr

Pages: 114-123 URL: https://doi.org/10.31703/gmsr.2025(X-III).11 Doi: 10.31703/gmsr.2025(X-III).11

Title

Beyond HIPAA: Rethinking Health Data Governance in the Age of Machine Learning

Abstract

With the spread of Machine Learning (ML) and Artificial Intelligence (AI) in the healthcare sector, the regulatory structures that currently dominate the field (particularly HIPAA law in the United States) have become unable to deal with emerging challenges and opportunities offered by health data utilization. This paper argues that the growing trend of predictive analytics and algorithmic evaluations needs governance models that go beyond the standard perimeter-centric and consent-based paradigm of HIPAA. By identifying key governance issues, such as algorithmic bias, data provenance, dynamic consent, federated learning architectures, and power asymmetries in the data ecosystems, the article suggests a multi-layered governance model, which should be based on the principles of accountability, fairness, transparency, data stewardship, and multi-stakeholder co-regulation. Along with the application of this model in clinical diagnostics, public health research, and business analytics, periodic reassessment of health data regulations is highly emphasized to protect health data privacy.

Keywords: Health Data Governance; Machine Learning; Hipaa Reform; Algorithmic Accountability; Data Stewardship; Privacy-Sensitive AI

Authors:

Ahmed Raza: (Corresponding Author)
LLM Scholar, Pennsylvania State University, USA.
Email: (ahmedraza.sajjad@gmail.com)

Shahzad Khalid: Doctoral Researcher, Brunel University London, United Kingdom.
Assistant Professor, Department of Law, Superior University, Lahore, Punjab, Pakistan.

Ali Nawaz Khan: Assistant Professor, University Law College, University of the Punjab, Lahore, Punjab, Pakistan.

Contents

- Introduction
- Dynamic Data and Model Drift
- Equity, Bias, and Distributional Harms
- Transparency and Dynamic Consent
- Multi-Institutional Federated Architectures
- Incentives, Power, and Data Monopolies
- Normative Analysis
- Technical Safeguards
- Infrastructure Oversight and Accountability
- Illustrations of Use-Cases and New Models
- Policy Routes to Post-HIPAA Governance
- Conclusion
- References

Introduction

The advent of ML and AI has brought an unprecedented change in the field of health informatics, making a revolution in clinical prediction, diagnostics, and management of health-systems (Ghassemi et al., 2021; Reddy et al., 2020). AI is actively used to analyze large amounts of electronic health records (EHRs), genomic profiles, and biometric streams to facilitate personalized care and predictive interventions to the population (Vayena et al., 2018). Radiology models, which have been trained on millions of images, can identify pathology with the level of accuracy as a human being and predictive algorithms show early signs of sepsis and cardiovascular events (Fenton, 2025). But the data substrate itself which drives this innovation has provided complicated governance difficulties never intended to be handled by conventional privacy legislation (Solove, 2025). Even though the U.S. Health Insurance Portability and Accountability Act (HIPAA) is historical, it was designed in a pre-AI setting where records were fixed and institutionalized

(AHIMA, 2023). It becomes more inappropriate to a learning ecosystem with an incessant flow of information spanning institutions and algorithmic inferences (Saheb & Izabi, 2023).

In this article, the authors question the shortcomings of the HIPAA and suggest a more wholesome framework regarding the reconsideration of health data governance in the context of the changing architecture of the machine learning (Raghupathi and Raghupathi, 2019; Jones et al., 2021). It promotes a paradigm shift on episodic compliance to continuous accountability which involves algorithmic auditing, dynamic consent and multi-stakeholder oversight (WHO, 2023). The discussion is divided into four stages, including the analysis of the structural limitations of HIPAA, key governance challenges recognition, the creation of the multi-layered governance structure, and policy/future research recommendations (O'Sullivan et al., 2023; Cambridge University Press, 2024). This way, it aims to place U.S. data law into the context of international ethical discussions of responsible AI and digital-health regulation (Mittelstadt, 2019; Vayena et al., 2018).

The Weaknesses of HIPAA in the Age of Machine Learning

HIPAA was signed in 1996 to secure the privacy of the patients and enable easy sharing of medical records with providers and the insurers (Reddy et al., 2020). Its Privacy and Security Rules formalized a concept of confidentiality and integrity, identifying what constitutes the protected health information and binding responsibilities on the so-called covered entities. However, the architecture of HIPAA is a symptom of a limited number of transactions and manual information sharing (AHIMA, 2023). The AI-based healthcare today is marked by both automated data fusion and predictive analytics as well as iterative model training, which recycles information between various settings (Saheb & Izabi, 2023). According to Jones et al. (2021), the categorical concepts of use and disclosure under HIPAA are unable to reflect the recursive nature of machine-learning pipelines, making its compliance structure a more and more symbolic than substantive construct.

Moreover, the jurisdiction of HIPAA ceases after the data are de-identified, which machine-learning methods can easily overcome by re-identifying and inferring (Zhao et al., 2023). The law only governs record-keepers but not model developers or artificial intelligence providers who tend to have a more significant impact on clinical decisions (Raza, 2024). In turn, HIPAA is a baseline of privacy as opposed to a universal governance regime in the age of algorithms.

Consent, Purpose limitation, and Secondary Use

The background of HIPAA in terms of consent and purpose restriction is the idea of privacy that is grounded in personal authorization (Solove, 2025). Nevertheless, machine-learning applications are regularly reusing the past data to do secondary tasks including predictive modeling and clinical research (O'Sullivan et al., 2023). Finding new consent by millions of patients at every instance of analysis is unfeasible (Ghassemi et al., 2021). In addition, the principle of the minimum necessary is incompatible with the nature of AI that requires granular and longitudinal data, which provides fine-grained correlations (Reddy et al., 2020). Data de-anonymization can commonly decrease the utility of analysis, which a researcher can refer to as a privacy-utility trade-off (Zhao et al., 2023). These strains reveal the conceptual ineptitude of HIPAA to cope with the ongoing purpose-adapting utilization of health data.

Business Associates and AI Vendors Role

The decision to extend the scope of HIPAA to business associates was an effort to encompass the subjects that conducted data-related operations on behalf of covered entities and thus sealing the loopholes on third-party liability (Saheb & Izadi, 2023). However, when applied to artificial intelligence, there is no longer a distinction between the processors and the controller. The vendors of AI are also poorly defined as hybrid in nature: they can be technical processors when training models for hospitals, but also as independent controllers when storing derived parameters or commercial use of trained models (Jones et al., 2021). This bidirectional role creates confusion on the matter of ownership, liability, and custodianship. Organizations that create algorithms using multi-institutional data often process raw data into predictor models which have separate economic and clinical utility. These models are typically trained on the secured health information (PHI), but once the data is abstracted into algorithmic weights or embeddings, they are beyond the scope of HIPAA, which leaves the question of whether the resultant learned representation is PHI (Liu and Chen, 2022).

The contractual tools that have served to regulate the relationships between the covered entities and the vendors are known as Traditional Business Associate Agreements (BAAs), which are ill-suited to the nature of machine learning. Such agreements are often concerned with data storage, transmission, and breach notification, but seldom consider the problem

of retraining an algorithm, sharing of parameters federally, or the entitlement to audit model performance due to bias (Jones et al., 2021). Consequently, a vendor can be left with some control over a developing model that keeps learning with the new streams of data without express management by the healthcare provider. It is further complicated by the fact that proprietary systems are not transparent enough, as vendors tend to use trade-secret regulations to avoid sharing training information, performance indicators, or the architecture of models (Mittelstadt, 2019).

The result is a governance gap whereby the responsibility of algorithmic harms (e.g., wrong diagnosis or controversial recommendation) is scattered among various actors. Although HIPAA outlines an accountability for breaches of data, it offers no similar accountability for algorithm malfunctions or discrimination (Saheb & Izadi, 2023). As an example, it implies that a patient harmed by an AI-driven decision may not find a path of redress. The situation is additionally complicated by the introduction of the so-called "AI-as-a-Service platforms", where the models trained on the data of a single hospital can be reused in others, which creates systemic latent biases (Ghassemi et al., 2021). Researchers have thus demanded a broadened concept of data stewardship that extends beyond the management of the raw information but also the control of the derivatives of algorithms. This would involve the contractual requirements that outline the explainability, validation, and post-deployment monitoring requirements that align the accountability of the vendor with the ethical requirement of clinical safety and equity (WHO, 2023).

Auditability, Transparency, and Algorithmic Accountability

The audit features of HIPAA are more suited to the case of a static database and access records, rather than the case of dynamic and learning-based systems, which change with ongoing retraining (Reddy et al., 2020). Its compliance paradigm is based on checking authorized access and encryption as opposed to questioning the logic about the algorithms (Liu and Chen, 2022). Conversely, contemporary healthcare AI creates both model and institutional opaqueness. Deep learning models, including convolutional neural networks with radiology applications or natural language processing systems with clinical documentation applications, use millions of parameters, which makes their internal logic impossible even for writers of their own code (Ghassemi et al., 2021). The interpretability of algorithmic decisions is a corporate responsibility and not a regulatory obligation without legally required standards of documentation, model cards, or validation datasets (Mittelstadt, 2019).

This non-transparency compromises major tenets of informed consent and due process. Clinicians who use algorithmic results are usually unable to say to patients why this or that diagnosis or risk score was generated, thus undermining the sense of trust and accountability (Liu & Chen, 2022). Moreover, there are no standardized audit systems in institutions to ensure the fairness of models or to allow the tracing of the effect of input data on predictions. Regulators have already started to demand explainability of algorithms as a prerequisite to market participation in other industries, including the financial industry; in healthcare, it is still lagging (Raza, 2024).

The solution to this gap is the introduction of algorithmic audits into health governance. These audits are necessary to integrate technical testing (e.g., bias testing, performance testing) with procedural testing (e.g., model documentation, governance testing, and stakeholder testing). Introducing the concept of model provenance logs and explainability documentation to the audit schema of HIPAA would bring the regulatory practice in line with the reality of machine learning. The lack of these innovations makes the statute stuck in a paper-era model of compliance, which is not suited to the algorithmic medicine (Saheb & Izadi, 2023).

Data Residency, Transfers across Borders, and Federated Learning

The territorial governance of HIPAA, which is limited to the United States, is another significant source of governance challenge in a globalized data environment (Jones et al., 2021). The contemporary healthcare is very dependent on the international cloud systems, distributed storage, and international research cooperation. Replication of the data with servers spread in several jurisdictions is a practice of cloud replication, which might conflict with the foreign privacy laws like the European Union General Data Protection Regulation (GDPR) (Cambridge University Press, 2024). Although HIPAA permits the application of offshore servers with a contract to prevent possible breaches, it does not provide extra-territorial application and regulatory framework harmony.

Furthermore, the emergence of federated learning, which is a practice of training common models at decentralized institutions without data transfer between them, also makes it more challenging to govern (Chen et al., 2019). Federated

learning has facilitated community-based AI development and preserved the local data privacy of the members; however, it has added novel points of risk: malicious updates, aggregation bias, and different institutional representation (Saheb & Izadi, 2023). An example is a hospital that is part of a federated consortium, and as such, it can change the behavior of the global model without full knowledge of how its updates are combined. The legal ownership of the resulting model, such as in individual contributors, the aggregator or the coordinating vendor, has not been defined in law.

The existing HIPAA does not envisage or regulate these trans-jurisdictional architectures. The legal system presumes that the possession of data is equal to the physical possession of the data, which is invalidated by the cloud and federated computing (Jones et al., 2021). With the globalization of research countenanced by utilizing common world data governance models, the United States stands to be in regulatory seclusion unless the HIPAA is amended to encompass global interoperability (WHO, 2023). The bilateral and multi-lateral agreements that acknowledge mutual standards of governance may address these gaps and provide ethical cross-border cooperation in health data research.

Dynamic Data and Model Drift

The machine learning models are based on the relevance of data over time (Abbasi et. al., 2025). Health data is dynamic in nature, diagnostic codes change, disease rates vary, and treatment plans change with medical development (Reddy et al., 2020). The model performance also declines with shifts in underlying data distributions, which is referred to as model drift (Liu and Chen, 2022). HIPAA, though does not place any condition on the continuous validation, recalibration or lifecycle management of predictive models. After an algorithm deployment, it can operate years without the compulsory performance review. The outcome is a governance gap that is characterized by adherence to privacy requirements and substantive clinical risk.

The observation and retraining must hence be the institutionalized element of the data governance (Ghassemi et al., 2021). Similar to post-market testing in medicine, health AI ought to be re-certified periodically in order to be safe and just. The regulatory agencies may make institutions have model registries and capture retraining events, and publish the performance indicators. In the absence of such protective measures, the outdated algorithms can continue to propagate the diagnostic errors, bias the risk estimations, or be systematically discriminative of a specific group of people (Mittelstadt, 2019). The systemic management of model drift, as a way of data governance, would serve as a way of aligning data management with the concept of nonmaleficence at the core of medical ethics.

Equity, Bias, and Distributional Harms

The machine learning systems replicate the social and historical biases within their training data, making the disparities in health status more pronounced in most cases (Mittelstadt, 2019; Liu & Chen, 2022). The privacy, which is the narrow concept of HIPAA, fails to cover the aspect of algorithmic fairness or auditing equity (WHO, 2023). Therefore, a model might still be in line with HIPAA and still promote systemic discrimination. Presumably, as it has been shown, an algorithm employed in healthcare resource allocation underestimated the needs of Black patients since expenditure data, as a proxy of illness severity, indicated past underinvestment in minority populations (Ghassemi et al., 2021). These inequalities are indicative that privacy guarantees are not enough to bring justice in data-driven healthcare.

The contemporary model of governance needs to entrench equity as a legal and ethical requirement. This is by incorporating bias diagnostics, subgroup performance reporting and remediation procedures at each phase of the machine-leaning pipeline. The regulators must make the composition of training data and the fairness measures a pre-requisite to the algorithmic certification (O'Sullivan et al., 2023). Furthermore, seeking the engagement of the populace in governance boards may serve to make the marginalized communities have a say in the regulation of their data. By governing the AI according to the principles of equity, one can turn the regulation into a social responsibility, instead of just complying with it (WHO, 2023).

Unintended Inferences and Re-Identification

The identifiability reaches much further than the trademarks with the assistance of the artificial intelligence. Sensitive features like genetic predisposition, mental disorder, or socioeconomic status can be determined by models based on apparently harmless data such as voice recordings or facial expressions (Vayena et al., 2018). This incidental conclusion shifts the boundary between the non-identifiable and identifiable data and makes the de-identification standards set by HIPAA irrelevant (Zhao et al., 2023). The historic erasure of 18 identifiers cannot resist re-identification in cases where advanced algorithms are able to rebuild identities using connection to other datasets.

It must therefore provide protection to derived data, such as embeddings, synthetic features, and inferred traits, that will not necessarily refer to specific persons, but nonetheless disclose sensitive information. PHI needs to be redefined to include these algorithmically generated representations and require risk-assessment protocols to be done in any model that can make inferences. In a world where this expansion has not been made, people are still exposed to discrimination and profiling despite their nominal identifiers being removed in datasets (WHO, 2023). The identification of inference as a specific threat to privacy is an important step in transforming the compliance of the statistical data protection to the active cognitive privacy.

Key Governance issues in Health ML Ecosystems

The shift to holistic data governance, as opposed to privacy compliance, brings with itself a suite of new problems, which interact at legal, ethical, and computational design levels (O'Sullivan et al., 2023). These issues are not merely indicators of the complexity of machine-learning processes, but they are also indicative of power and knowledge asymmetries that constitute the digital-health economy (Jones et al., 2021). To establish a proper governance system, these structural barriers must be tackled in an orderly manner.

Versioning, Lineage and Data Provenance

Quality governance relies on the ability to track the data lineage. Health data are processed through many changes, including the process of data collection, cleaning, normalization, feature extraction, and all of them may be biased or unclean (Saheb & Izadi, 2023). There can be no accountability of model behavior without formal documentation of provenance (Raghupathi & Raghupathi, 2019). Lack of version control may result in cases where forecasting is done using obsolete or distorted data, making regulatory inspections as well as the reproducibility of science harder (O'Sullivan et al., 2023). Standardized metadata, unalterable logs, and audit trails would therefore form the foundation of transparency at the infrastructural level, allowing regulators as well as institutions to retrace the entire history of the development and application of a model.

Transparency and Dynamic Consent

Classical form of static consent fails in perpetual reuse of the data (Solove, 2025). Patients usually grant the consent to use their data to deliver clinical services in the nearest future, not to provide secondary analysis or train the algorithms indefinitely. Dynamic consent provides a participatory framework which enables individuals to revoke, amend, and track data processing and withdraw permission over time (Kaye et al., 2018). The use of dynamic consent is associated with the availability of interoperable digital infrastructure and transparent and accessible communication regarding AI applications (Ghassemi et al., 2021). It would be possible to establish trust and legitimacy by introducing transparency portals that explain to patients the ways and places of how their data are used in algorithmic processes (WHO, 2023). Formalizing these systems would engage autonomy in a manner that is aligned to the law and ethical demands (Raza, 2024).

Multi-Institutional Federated Architectures

Federated learning makes it possible to collaboratively model without storing sensitive information in one place (Chen et al., 2019). Although promising, they create new governance dilemmas such systems generate. The participating institutions cannot be equally endowed with equal computational resources resulting in disproportionate contribution to the aggregate model (Cambridge University Press, 2024). In addition, malicious or poorly set up nodes may provide so-called poisoned updates, which impairs the performance or ciphers bias (Saheb & Izadi, 2023). The governance frameworks should lay clear guidelines on membership, weighting of contribution and ownership of models. It should be aggregated transparently, audited, and involve itself and others equally to avoid some kind of data colonialism, whereby well-funded organizations control the world-health consortia (WHO, 2023).

Accountability, Auditability and Explainability

The accountability also demands the intelligible nature of the algorithmic decisions to the clinicians, patients, and regulators (Liu & Chen, 2022). The explainability methods, including SHAP values or counterfactual inferences, should be part of clinical AI pipelines (Ghassemi et al., 2021). The lack of formalized audit mechanisms can lead to the spread of errors without being noticed, and the victims have no means to do so (O'Sullivan et al., 2023). The governance must mandate the ongoing documentation of models, versioning models and evaluating the interpretability of models. Making auditability embedded in the technical infrastructure and policy instability allows implementing the algorithmic systems that are not only accurate but also justifiable (Mittelstadt, 2019; Raza, 2024; Munir et. al., 2025).

Bias Detection, Remediation and Algorithmic Fairness

Ethical AI is based on fairness and the existing legal frameworks can offer only slight operational guidance (Mittelstadt, 2019). The governance should enforce fairness reviews in the model development and implementation (Liu & Chen, 2022; Munir et al., 2025). Inequality can be measured by metrics like equalized odds or demographic parity, but to fix it, organizations must be dedicated and intervention of policy is necessary. Organizations are encouraged to record remedial measures be it the addition of data, adjusting algorithms, or redistribution of funds, and publish the result for everyone to see. Associating the procurement or accreditation with the fairness performance would make equity a compliance institutionalized measure (WHO, 2023).

Incentives, Power, and Data Monopolies

Big technology companies have combined health data and computer power to generate new types of informational monopoly (Jones et al., 2021). These imbalances allow the private actors to establish a de facto rule, usually serving proprietary interests in spite of patient interests (Saheb & Izadi, 2023). To offset this concentration, systems of governance should be aimed at facilitating collaborative data trusts and partnerships of the public interest that share power in an equitable way (Raghupathi & Raghupathi, 2019). By refocusing incentives on openness, interoperability, and social good, it is possible to make sure that the data are used to fulfill the goals of collective health, rather than achieving corporate goals (WHO, 2023). The difficulty is both political and technical in nature, i.e. building a government that democratizes information and protects individual liberties.

Toward a Multi-Tiered Governance Model

To regulate the use of machine learning in healthcare, there is a need to have a systemic framework, which functions at the same time in normative, institutional, technical, and oversight levels (O'Sullivan et al., 2023). Ethical principles are not sufficient to guarantee adherence, and they have to be incorporated into the institutional mechanisms and technological infrastructures (Mittelstadt, 2019). The model presented here incorporates normative commitments, organizational implementation, technical safeguards, and independent accountability (WHO, 2023).

Normative Analysis

Successful governance is built on a basis of shared values that arbitrates innovation and mistrust of people. The issue of accountability and stewardship implies that the individuals handling health data should be aware of a long-term responsibility of care (Solove, 2025). The transparency and explainability once more provide interpretability of algorithms and make them contestable (Liu & Chen, 2022). Fairness requires continuous performance appraisal among demographic groups (Ghassemi et al., 2021). The principles of privacy and data minimization require institutions to limit collection and to use privacy-preserving methods including different privacy, and federated learning (Chen et al., 2019). The principle of beneficence requires AI implementation to promote clinical and social good instead of institutional efficiency (WHO, 2023). Participatory co-governance incorporates the views of the patients whereas adaptivity recognizes that governance needs to adapt as technology and risk are changing. All these principles comprise a normative guide for the post-HIPAA governance ecosystem.

Institutional and Organizational Mechanisms

The principles should be operationalized by institutionalization of governance in healthcare organizations. The presence of data stewardship offices and multi-stakeholder boards is a way to be able to control the lifecycles of algorithms (Jones et al., 2021). The existence of formal model-use agreements is the definition of responsibilities, the necessity of fairness audit, and the right to access the external review (Saheb & Izadi, 2023). The incentive of compliance could be provided by accreditation and reimbursements programs that encourage open and fair practices (Reddy et al., 2020). The compliance with the governance standards should be evaluated by independent certifiers, and governance-as-code in the digital infrastructure ensures compliance by design (Ghassemi et al., 2021). Institutionalization turns abstract ethics into organizational culture which is enforced.

Technical Safeguards

Governance principles need to be captured in technical design. End-to-end data and model transformations are tracked through provenance and immutable logging (Saheb & Izadi, 2023). The re-identification risk is minimized with the help of differential privacy, homomorphic encryption, and secure computation methods (Zhao et al., 2023). Federated learning models encourage joint modeling without the centralization of sensitive data (Chen et al., 2019). The interpretability of a model can be

achieved through explainability modules like model cards and feature-importance visualizations (Liu & Chen, 2022). Bias-reducing constraints are introduced in fairness-conscious algorithms, and the model is continuously monitored to identify model drift and decreasing performance (Ghassemi et al., 2021). Comparatively, they make Governance as an inherent measure of the system's architecture instead of enforcing a constraint (Mittelstadt, 2019).

Infrastructure Oversight and Accountability

The formulation of governance should result in the independent oversight that implements transparency and accountability (WHO, 2023; Munir, 2025). All algorithmic decisions must be logged in comprehensive audit trails to allow them to be reviewed by a third party (Reddy et al., 2020). Fairness and safety are evaluated by independent audits which result in the public certification of reliable systems (O'Sullivan et al., 2023). Recourse mechanisms allow patients and clinicians to challenge the results of algorithms, which guarantees procedural justice (Solove, 2025). Performance and incidents of the models are reported on a regular basis, and incident-response procedures provide institutions with the authority to suspend unsafe systems. The regulatory sandboxes are able to facilitate controlled experimentation with new governance instruments, and accreditation programs are able to establish tiered trust programs to compliant organizations (Mittelstadt, 2019; WHO, 2023). With this kind of infrastructure, control will be persistent and enforceable, and a sense of ethical accountability will be incorporated into the technical and institutional composition of healthcare AI.

Implementation Constraints and Barriers of an Institution

Although there is an increasing agreement that post-HIPAA reform is necessary, it has not been fully implemented because of the scattered power, institutional inertia, and unequal technical capacity (Jones et al., 2021; Saheb & Izadi, 2023). The digital maturity of healthcare organizations is also very diverse: tertiary hospitals can have open-source AI pipelines; community clinics continue to use ancient systems (Reddy et al., 2020). This imbalance makes it difficult to have uniform governance. In addition, the HIPAA compliance departments typically belong to a legal or administrative department that lacks familiarity with algorithmic audits or fairness measures, and they present a disparity between policy and practice (O'Sullivan et al., 2023). Numerous institutions do not have anyone to make sense of bias reports or add explainability tools to clinical workflows (Liu & Chen, 2022). The non-appearance of cross-disciplinary literacy, that is, the connection of data science, law, and ethics, therefore, disadvantages the implementation of governance.

Reform is also hampered by economic and political incentives. Vendors of AI sell their efficiency and cost-saving, and hospitals are pressured to implement the models in advance without proper oversight systems in place (Mittelstadt, 2019). Commercial secrecy can also be a problem with revealing training data or algorithmic logic and limits transparency. Moreover, the trend of ongoing audits and certification may prevent the smaller providers, which results in a gap between the systems with adequate funding and those with inadequate resources (Ghassemi et al., 2021). The government should therefore invest resources and expertise in democratization of the compliance infrastructure through public policy (WHO, 2023). Lastly, the overlapping in accountability and gaps in mandates between federal and state agencies, HHS, FDA, FTC, and state privacy commissions, are brought about by regulatory fragmentation (Solove, 2025). This regulatory disagreement would be addressed through harmonized federal leadership perhaps by establishment of a national Health Data Governance Authority.

Illustrations of Use-Cases and New Models

Experiments in ethical AI governance have shown both their strength and weakness at an early stage. The collaboration between the DeepMind and the National Health Service to predict kidney-injury also triggered a public backlash in the United Kingdom with regards to the lack of transparency in data sharing, which serves to demonstrate how such partnerships need to be transparent and involve patients (Jones et al., 2021). Conversely, the Scottish model of co-governance, in which controlled settings allow approved researchers and pseudonymized data, the so-called Safe Haven (Kaye et al., 2018), is an example of a model consistent with the public interest. Pilot programs in federated learning in oncology diagnostics have been demonstrated in the United States, and institutions can be trained to collaborate without data pooling (Chen et al., 2019). These initiatives demonstrate technical capability of privacy preserving analytics and also provide indications of continued governance gaps in terms of accountability of global model outputs (Cambridge University Press, 2024).

The limits of HIPAA are also complicated as shown by the private-sector projects. The Project

Nightingale by Google and Ascension Health partnership, despite being compliant as per the provisions of HIPAA, business-associate, created ethical dilemmas concerning business access to sensitive data (Project Nightingale Case Study, 2024). The episode revealed the conflict between the formal and the substantive trust. On the other hand, transparency and reproducibility do not have to be incompatible with privacy when such open-source consortia as the Observational Health Data Sciences and Informatics (OHDSI) network show that they can be implemented in a transparent and reproducible way (O'Sullivan et al., 2023). Combined, these case studies show that the success of governance is not only based on the adequacy of the legal but also on social legitimacy, which is grounded in the consent, communication and community involvement (WHO, 2023).

Policy Routes to Post-HIPAA Governance

The reform of policies should not be based on some minor improvements to HIPAA but a complete governance regime that incorporates accountability through algorithms, equity, and innovation (Solove, 2025). One of these paths is the adoption of a federal Health Data Governance Act that would require minimum requirements of algorithmic documentation, bias audit, and transparency reporting (Reddy et al., 2020). This legislation must work alongside and not duplicate the current HIPAA safeguards, including derived data, created datasets, and AI sellers outside the customary covered-entity barrier (Jones et al., 2021). Adaptive standards may help to create regulatory flexibility: every period, standards are to be updated to reflect the technological changes, which is similar to the Software as a Medical Device (SaMD) framework created by the FDA (Liu & Chen, 2022).

The second route is the enhancement of institutional governance. The federal grants and accreditation programs may make the funding depend on the achievement of the governance norms including dynamic consent, open model documentation, and the involvement of external auditors (Ghassemi et al., 2021). The association of professionals such as AHIMA and the American Medical Informatics Association may publish revised codes of practice to align the data management with AI ethics (AHIMA, 2023). It is also important that HHS, FDA, and NIST cooperate with one another: the standard technical requirements related to model validation, security, and interoperability can be unified (Saheb & Izadi, 2023). Lastly, cross-border research would be more straightforward with global alignment with GDPR and the OECD AI Principles, which would further provide mutual privacy protection (Cambridge University Press, 2024; WHO, 2023). These reforms would change governance reactive compliance rather than proactive accountability.

Governance of Health Machine Learning; A Research Agenda

Health data governance is an area of practice that is not yet empirically and conceptually developed. Further studies are needed into the role of governance in influencing the patient trust, clinical and innovation rates (O'Sullivan et al., 2023). Longitudinal studies would be able to test the hypothesis that dynamic-consent systems enhance the diversity of participation and quality of data (Kaye et al., 2018). Coming up with comparative studies of jurisdictions, e.g. the European GDPR regime and the U.S.-based HIPAA regime, would make the trade-offs between stringent legal control and flexible regulation more visible (Jones et al., 2021). Technical scholarship needs to keep improving the privacy-preserving machine-learning models like the one that is known as differential privacy, homomorphic encryption, and federated aggregation (Chen et al., 2019; Zhao et al., 2023). Meanwhile, the analysis of the role of the organization culture in mediating the application of the governance tools requires the social-science inquiry (Mittelstadt, 2019).

The concept of algorithmic due process must be formulated by ethics and legal experts in healthcare, establishing procedural rights of people impacted by the automated decision (Solove, 2025; Munir et al., 2025). It is also essential to evaluate the bias-reducing methods in diverse populations through empirical means to make sure the systems of governance promote distributive justice (Liu and Chen, 2022). Lastly, interdisciplinary cooperation, i.e., integrating law, medicine, computer science, and sociology, should become the new methodological standard of analyzing algorithmic health governance (WHO, 2023). Unless such integrative scholarship is present, reform risks slipping into technocratic minimalism instead of transformative accountability.

Conclusion

With the growing use of machine learning and artificial intelligence in the field of medicine, it has significantly demonstrated the inefficiencies of current privacy legislation dealing with healthcare system. HIPAA is configured to handle inert information setting, which is not adaptable to the dynamic, iterative, and inferential environment of contemporary health

information. As it has been demonstrated in this article, effective governance for the modern healthcare system requires a multi-layered coordination of ethical principles, institutional mechanisms, technical design, and independent oversight. To attain legitmacy, it is further crucial to ensure that the post-HIPAA paradigm should embed transparency and fairness in it as its core values. These reforms will also require innovative regulation, investment within the organization, and interdisciplinary experience. For these reforms, the reward, which is a reliable and fair digital healthcare system, definitely justifies the efforts. Along with this, the incorporation of accountability in legal and digital spheres can help society to hold intelligent systems accountable, beneficial, and safe for the human use.

References

Abbasi, M. S., Munir, B., Jayaram, V., & Rivas, P. (2025). Leveraging autocorrelation in a dilated CNN-LSTM framework for predicting the US Supreme Court decisions. *IEEE Access.*
Google Scholar Worldcat Fulltext

American Health Information Management Association (AHIMA). (2023). Updating HIPAA security to respond to artificial intelligence. *Journal of AHIMA.*
Google Scholar Worldcat Fulltext

Cambridge University Press. (2024). Operationalizing health data governance for AI innovation in low-resource government health systems: A practical implementation perspective from Zanzibar. *Data & Policy. 6*(2). e15.
Google Scholar Worldcat Fulltext

Chen, Y., Wang, J., Yu, C., Gao, W., & Qin, X. (2019). FedHealth: A federated transfer learning framework for wearable healthcare. *IEEE Intelligent Systems, 35*(4), 83–93. https://doi.org/10.48550/arXiv.1907.09173
Google Scholar Worldcat Fulltext

Ghassemi, M., Naumann, T., Schulam, P., Beam, A. L., Chen, I. Y., & Ranganath, R. (2020). A Review of Challenges and Opportunities in Machine Learning for Health. *AMIA Joint Summits on Translational Science proceedings. AMIA Joint Summits on Translational Science*, *2020*, 191–200.
Google Scholar Worldcat Fulltext

Jones, K. H., Laurie, G., & Stevens, L. (2021). Governance of data and artificial intelligence for health care: A UK perspective. *Computer Law & Security Review, 43,* 105618.
Google Scholar Worldcat Fulltext

Kaye, J., Curren, L., Anderson, N., Edwards, K., Fullerton, S. M., Kanellopoulou, N., Lund, D., Macdonald, A., & Mascalzoni, D. (2018). Dynamic consent: A patient interface for twenty-first-century research networks. *European Journal of Human Genetics, 26,* 141–149. https://doi.org/10.1038/ejhg.2014.71
Google Scholar Worldcat Fulltext

Liu, V. X., & Chen, I. Y. (2022). Algorithmic fairness in healthcare: Practical challenges and lessons learned. *The Lancet Digital Health, 4*(8), e600–e612. https://doi.org/10.1038/s41551-023-01056-8
Google Scholar Worldcat Fulltext

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence, 1,* 501–507. https://doi.org/10.1038/s42256-019-0114-4
Google Scholar Worldcat Fulltext

Munir, B. (2025). *Artificial intelligence for lawyers: Navigating novel methods and practices for the future of law.* Punjab Law Book House.
Google Scholar Worldcat Fulltext

Munir, B., Abbasi, M. Z., Wilson, W. B., & Colombo Jr, A. (2025). Evaluating AI in legal operations: A comparative analysis of accuracy, completeness, and hallucinations in ChatGPT-4, Copilot, DeepSeek, Lexis+ AI, and Llama 3. *International Journal of Legal Information,* 1–12. https://doi.org/10.1017/jli.2025.10052
Google Scholar Worldcat Fulltext

Munir, B., Khalid, S., & Noreen, U. (2025). EXPOSING ISLAMOPHOBIA IN MACHINE LEARNING: A CRITICAL ANALYSIS OF THE EXISTING THEORIES AND BIASES. *Center for Management Science Research*, *3*(3), 1-9.
Google Scholar Worldcat Fulltext

O'Sullivan, D., Rahim, M. F., & Sujan, M. A. (2023). Governing AI in healthcare: A review of the evidence and recommendations for policymakers. *Health Informatics Journal, 29*(1), 1–20. https://doi.org/10.2196/31623
Google Scholar Worldcat Fulltext

Project Nightingale Case Study. (2024). Data governance in AI-enabled healthcare systems: The case of Project Nightingale. *Asian Journal of Research in Computer Science, 13*(2), 32–48. https://doi.org/10.9734/ajrcos/2024/v17i5441
Google Scholar Worldcat Fulltext

Raghupathi, W., & Raghupathi, V. (2019). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems, 2*(3), 1–10. https://doi.org/10.1186/2047-2501-2-3
Google Scholar Worldcat Fulltext

Raza, A. (2024). Beyond HIPAA: Legal challenges in the governance of AI-driven healthcare data. *Center for Multidisciplinary Scientific Research Journal, 5*(1), 45–62.
Google Scholar Worldcat Fulltext

Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. *Journal of the American Medical Informatics Association: JAMIA, 27*(3), 491–497. https://doi.org/10.1093/jamia/ocz192
Google Scholar Worldcat Fulltext

Saheb, T., & Izadi, M. (2023). Evaluating the effectiveness of data governance frameworks in healthcare. *Health Information Science and Systems, 11*(17), 1–15. https://doi.org/10.1371/journal.pone.0324285
Google Scholar Worldcat Fulltext

Solove, D. J. (2025). *Understanding privacy in the age of AI and health data.* Yale University Press. https://dx.doi.org/10.2139/ssrn.4713111
Google Scholar Worldcat Fulltext

Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. *PLoS medicine*, *15*(11), e1002689. https://doi.org/10.1371/journal.pmed.1002689
Google Scholar Worldcat Fulltext

World Health Organization (WHO). (2023). *Guidance on ethics and governance of artificial intelligence for health.* World Health Organization.
Google Scholar Worldcat Fulltext

Zhao, J., Papin, J. A., & Wang, W. (2023). Data privacy in healthcare: In the era of artificial intelligence. *Frontiers in Digital Health, 5*(1223), 1–17.
Google Scholar Worldcat Fulltext