if available

THE FIRST INTERNATIONAL CONGRESS ON HEALTH SERVICES TRANSFORMATION

اولین کنگره بین المللی تحول خدمات سلامت

۲۷ و ۲۸ مهر ماه

ISC 05251-58426 Scopus CIVILICA



Applications and Implications of Artificial Intelligence in Health Data Governance: A Scoping Review of Ethical, Legal and Operational Challenges

Code: 1603

Mina Anvari(1), Shima Anvari*(2), Reihane Sharif (3), Reza Abbasi(4), Nafiseh Jamal(5)

1. Department of Health Information Management, School of Health management and Information Sciences, Iran University of Medical sciences, Tehran, Iran.
2. Health Information Management Research Center, Kashan University of Medical Sciences, Kashan, Iran.
3. Health Information Management Research Center, Kashan University of Medical Sciences, Kashan, Iran.
4. Department of Health Information Technology, School of Paramedical Sciences, Torbat Heydariyeh University of Medical Sciences, Torbat Heydariyeh, Iran.
5. Health Information Management Research Center, Kashan University of Medical Sciences, Kashan, Iran.

Backgrounds

The spread of artificial intelligence (AI) across health systems is reshaping health data governance: AI consumes health data, generates derived data, and increasingly serves as a governance instrument itself. Yet the evidence is scattered across disciplines and lacks an integrated map. This study therefore aimed to map the applications and implications of AI in health data governance and the associated ethical, legal, and operational challenges.

Methods

This scoping review followed the JBI framework and PRISMA-ScR reporting guidance. PubMed/MEDLINE and Scopus were searched through 27 September 2026, yielding 1,005 records, of which 211 documents were included. Documents were coded by the role of AI (governance tool or governance object), data governance dimensions, challenges, and proposed solutions.

Findings

Seventy-two percent of documents were published between 2024 and 2026. AI functioned as a governance tool, chiefly for de-identification, in 49% of documents, but as an object of governance in only 9%. Privacy was examined in 154 documents, whereas ownership and control (10) and secondary use (12) received little attention. Legal, ethical, and organizational challenges were the most frequent, yet proposed solutions were predominantly technical; auditing, stakeholder participation, and impact assessment were least represented. Field-based evidence constituted only 13% of the corpus, and no document originated from Iran in the searched databases.

Table 1. Ethical, Legal and Operational Challenges of AI in Health Data Governance

Domain	Theme	Problem Description	No. of Documents	Illustrative Sources
Legal / regulatory	Legal basis and gaps	Ambiguity in the legal basis for processing and secondary use in model training; misalignment between national and cross-border regulations; interaction of data-protection law with AI legislation; and unclear legal liability for errors.	117	[S071, S130, S003, S157]
Ethical	Consent, justice, and data misuse	Insufficiency of broad consent for unforeseen uses; re-identification risk; bias and inadequate representation of groups; and data colonialism in international collaborations.	91	[S139, S161, S118]
Organizational / operational	Policy-to-implementation gap	Absence of operational processes to enact principles; shortages of resources and specialized staff; workflow complexity; and weak system interoperability.	89	[S109, S159, S201]
Skills / capacity	Data and AI literacy	Need to redesign professional education and AI literacy for health and data-management staff.	72	[S131, S136, S018]
Transparency / explainability	Black box and standardization	Difficulty in explaining model decisions; lack of data and model standardization; and uncertainty about data provenance and authenticity.	66	[S094, S044]
Trust / acceptance	Patient and public perceptions	Governance contingent on public trust; differing patient attitudes toward data sharing with the public versus private sectors.	52	[S114, S026, S027]
Technical / infrastructural	Data silos and scalability	Heterogeneous formats; weak computational infrastructure; and difficulty scaling privacy-preserving solutions.	50	[S133, S178]
Security / privacy	Re-identification and threats	Vulnerability of anonymization methods to re-identification attacks; and security threats arising from generative AI.	43	[S070, S115]
Equity / inequity	Capacity and representation gap	Concentration of data and capacity in high-income countries, and the risk of reproducing inequity in models and in governance rules.	27	[S161, S180, S191]
Quality / representativeness of data	Validity of input data	Unvalidated datasets, incompleteness, and bias in training data framed as a governance issue rather than a merely technical one.	25	[S159, S094, S028]

Table 2. Proposed Solutions and Recommendations by Type and Target Challenge

Solution / Recommendation	Type	Challenge Addressed	No. of Documents	Level of Detail of the Evidence
Privacy-preserving technical mechanisms: de-identification, synthetic data, federated learning, homomorphic encryption; secure research environments	Technical	Privacy; secondary use	112	Mostly specific measures tested in experimental settings
Governance frameworks and principles (maturity models, guidance, by-laws)	Organizational / policy	Accountability; transparency; policy-to-implementation gap	69	Mostly general principles; less often accompanied by implementation metrics
Standardization and harmonization (common data models, metadata, FAIR principles)	Technical / organizational	Data quality; standardization	51	Specific measures at the infrastructure level
Education and capacity building (AI literacy, curricula, staff training)	Educational	Skills / capacity; trust	25	Mostly general recommendations
Audit, monitoring, and accountability mechanisms	Organizational / regulatory	Accountability; oversight	16	Sparse, and mostly propositional
Stakeholder and public engagement (co-design, public consultation, data trusteeship)	Social / governance	Trust; legitimacy	14	Sparse; limited operational examples
Policy and regulation (law reform, regulatory sandboxes)	Policy	Regulatory gaps	11	At the level of policy recommendations
Risk and impact assessment (DPIA, algorithmic impact assessment, compliance assessment)	Regulatory	Risk; compliance	8	Lowest frequency; mostly references to legal obligations

Conclusion

Institutional challenges are met largely with technical responses. Health data governance in the AI era cannot be reduced to de-identification; questions of licensing, accountability, and patients' share of data benefits demand institutional answers.

References

1. Guo LR, Liu S. The governance of health data in the AI era: a scoping review and computational topic model of the global research landscape. JAMIA open. 2026 Jun;9(3):ooag074.
2. Moulaei K, Akhlaghpour S, Fatehi F. Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review. International Journal of Medical Informatics. 2025 Jun 1;198:105872.
3. Faustini P, McIver A, Sullivan R, Dras M. De-identification of clinical data: A systematic review of free text, image and tabular data approaches. International journal of medical informatics. 2025 Dec 19:106225.