

Indian Journal of Modern Research and Reviews

This Journal is a member of the '*Committee on Publication Ethics*'

Online ISSN:2584-184X



Research Article

AI in Healthcare: Governance and Security Challenges

Vaibhav Bhosle

Department of Science and Technology, Shivaji University, Kolhapur, India

Corresponding Author: * Vaibhav Bhosle

DOI: <https://doi.org/10.5281/zenodo.22843754>

Abstract

AI has been implemented within healthcare to perform tasks such as medical image analysis, disease progression prediction, patient care communications, and administrative support. They may increase efficiency and reliability for a particular task; however, they are prone to regulatory issues due to privacy concerns with patient data; they can also generate mistakes that are not immediately obvious. The paper discusses issues related to management and safety concerns for AI healthcare systems during all phases of their existence. Privacy issues, data security concerns, fairness issues, transparency problems, accountability problems, cyber threats, and operational monitoring. Based on these issues, a five-stage governance framework is proposed: identification and risk classification, assessment before deployment, establishment of controls, operational monitoring, and review or retirement. Responsibilities are assigned to clinical staff, technical staff, privacy officers, legal advisors, compliance officers, management personnel, and patients' care providers. This article states that approval for deployment is inadequate. The healthcare AI needs to be monitored for changes to information, algorithms, programs, processes, and medical applications. Thus, it is a managerial task that involves patient care and security issues; it also includes suspending/withdrawing AI systems if needed.

Manuscript Information

- ISSN No: 2584-184X
- Received: 07-08-2026
- Accepted: 12-09-2026
- Published: 19-09-2026
- MRR:4(9); 2026: 200-203
- ©2026, All Rights Reserved
- Plagiarism Checked: Yes
- Peer Review Process: Yes

How to Cite this Article

Bhosle V. AI in Healthcare: Governance and Security Challenges. Indian J Mod Res Rev. 2026;4(9):200-203.

Access this Article Online



www.mrrjournal.in

KEYWORDS: artificial intelligence, healthcare, AI governance, cybersecurity, patient privacy, clinical decision support.

I. INTRODUCTION

AI has been adopted by health care institutions for information management, disease diagnosis and treatment decisions, and administrative tasks. Current applications include medical image analysis support; identification of patients at risk for deterioration; drug discovery activities; and selected administrative tasks. These tools are especially useful if there is a shortage of doctors' time and staff members' availability.

Governance needs differ to those of an ordinary information system. AI healthcare could affect diagnosis, treatment, triage and access to care for patients with sensitive medical data. A bad result, a security breach, a biased algorithm, or misuse of it outside its intended use would affect both patients and organisations running this software.

The article discusses healthcare AI from a combined perspective of governance and security. How does a company ensure that it has proper controls for safety, fairness, transparency, privacy and cybersecurity during all stages of AI development? This proposal links technology evaluation and specific organisational duties so that AI governance isn't just one approval process.

II. AI Applications in Healthcare

AI healthcare applications have been utilised and researched for various purposes. Medical imaging can help to detect abnormalities through radiology, pathology, ophthalmology, and dermatology images with the help of algorithms. Predictive models can be used by clinical decision support systems for identifying patients who are likely to deteriorate and need more attention. Other uses are patient-specific treatment plans; drug development; recruitment of participants to clinical trials; chatbot support for patients; appointment scheduling; medical coding; and public health monitoring.

They do not have equal risks. A tool to schedule appointments reminders will have an entirely different effect compared with one that suggests treatments and prioritises patients' needs. Therefore, governance should be based on purpose and risk for every AI system rather than having one set of rules that applies to all systems.

III. Governance Challenges

A. Privacy and Data Protection

Healthcare AI may need access to electronic health records, medical images, genetic information, insurance information, and data generated by patients through applications or connected devices. It is a risk of unauthorized access; re-identification of supposedly anonymous data; unnecessary collection; secondary use of information; and inadequate transparency from vendors. The data governance policy should define what data will be collected; authorised users; how long it will remain available for use; consent requirements; secondary uses allowed by it; and deletion conditions.

B. Bias and Equity

Model performance may differ among patients if its training set is not representative enough for that particular group where it

will be used to operate. Variations may be due to incomplete information; differences between past and present access to healthcare; trends observed from historical records; labels not representing target populations. Thus, evaluation must be concerned with performance of a given group, age, sex, ethnicity, language, disability, geography, and socioeconomic status. Performance aggregation might hide important differences for clinical application.

C. Transparency and Explainability

Healthcare professionals need adequate knowledge about what an AI is doing for them; how they tested it; and when its results might not work correctly enough. The system documentation must describe characteristics of data sets used for training; performance metrics; known limitations; uncertainties; and applications beyond those permitted by law. Information regarding how AI contributes to patient care should also be provided by means of language that they are familiar with.

D. Accountability

Healthcare AI accountability may include developers, healthcare organisations, doctors/clinicians, data providers, and vendors. Governance should not allow for ambiguous responsibilities post-incident. Every deployed system must also have an owner with an identity for approval; reporting and investigation procedures; suspension and withdrawal mechanisms if it's not appropriate to continue with it.

IV. Security Risks

Healthcare AI is vulnerable to traditional cybersecurity threats and also machine learning risks. A data breach might reveal patient data and the dataset used for training an AI model. Data poisoning is about injecting bad samples during the training process. Adversarial attacks may change an ML model's behaviour, for example by altering its input data (such as medical images). A model-extraction attack may try to recreate your own machine learning algorithm by making several requests. Generative AI also has risks like prompt injection and inappropriate disclosure of information.

Security controls must cover all of its technical infrastructure. Relevant assets are data sets, source code; applications; interfaces with health care systems; cloud computing services; medical equipment; customers; and vendors. Least privilege access, multifactor authentication, encryption, secure development practices, audit logging, dependency management, vulnerability testing, backups, and incident response procedures are some of them.

A security evaluation should not stop with approval of an organization's software product. Changes such as altering models and data sets; changing software; altering clinical workflows; modifying environments may affect risks associated with this model. Therefore, testing and reviews must also be repeated if there are any modifications made there.

V. Proposed Governance Framework

The proposed governance approach consists of five connected stages.

1. Identify and classify: Maintain an inventory of AI systems used by the organisation. Every system must then be categorised based upon things like threat to health and safety; data sensitivity; level of automation; possibility for discrimination; and reversibility.
2. Assess before deployment: Before deployment, conduct clinical validation, privacy and algorithmic impact assessment, cybersecurity testing, fairness analysis, human factors evaluation, and vendor due diligence. Assessment depth should be proportional to the identified risks of a given system.
3. Establish controls: Define user permissions, data-retention requirements, circumstances requiring human approval, disclosure practices, audit logging, backup procedures, and incident-response plans. They must also be documented prior to implementation.
4. Monitor in operation: After deployment, monitor accuracy, false-positive and false-negative behaviour, performance across patient groups, data drift, security events, clinician overrides, complaints, and patient-safety incidents. The monitoring gives information on whether this system is still operating as per its specifications.
5. Review or retire: Review and retire a system after major modifications and set out clear standards for suspension or withdrawal. Retirement is needed if it is no longer safe to operate; if there are biases that cannot be tolerated; if it's outdated; and no longer needed medically.

VI. Roles and Responsibilities

Healthcare AI governance involves coordination of various departments. The senior management sets up a company's risk appetite and provides necessary funds to carry out management functions. Healthcare leaders evaluate clinical significance and safety of practice. Privacy and consent are reviewed by data protection officers. The cybersecurity professionals deal with network security, architecture models, interfaces, and pipelines. Model design, operating conditions and limitations are documented by a developer. Legal and compliance professionals understand relevant regulations and contracts. Patients and those affected by them may offer feedback on acceptable applications for artificial intelligence.

The management committee is able to coordinate this task within an organisation. It might involve keeping track of AI registrations; approving risky projects; reviewing surveillance data; investigating incidents; and having powers to halt an unsafe implementation. The clear assignment of these roles

decreases the chances for critical government functions to be unowned.

VII. DISCUSSION

Accuracy is one thing that measures how well an artificial intelligence model performs, but it does not guarantee that it's suitable to use with medical diagnosis and treatment. A model which performs well within a controlled setting may not work as effectively if there are changes to patients' needs, alterations in procedure and technology, and poor data quality. Therefore, governance should be able to link technical assessment and usage conditions of a system.

Oversight of humans is especially critical when it comes to medical decisions that have serious ramifications. The clinician needs to know about AI systems; they must be able to question results; have a way of overriding those outputs; and report issues with them. Effective supervision is not just about assigning someone else's job. The employees must have enough education and opportunity for questioning a recommendation given by an artificial intelligence system if necessary.

VIII. CONCLUSION

Healthcare AI is capable of supporting medical and administrative tasks; however, it needs regulation which goes on after approval. Risk classification; data privacy; clinical validation; bias testing; human oversight; cybersecurity; operational monitoring; retirement when it is no longer justified.

This paper's model views AI governance as an ongoing organisational task. It's not about removing responsibility for patients' health care from humans, but ensuring that artificial intelligence is still under supervision by people and organisations. Future research may explore ways to apply such controls within organizations that have limited resources; it may also be possible to evaluate governance programs based upon actual outcomes for patients (health status), equity issues, and trustworthiness rather than just compliance with procedures alone.

REFERENCES

1. World Health Organization. *Ethics and governance of artificial intelligence for health: WHO guidance*. Geneva: World Health Organization; 2021.
2. World Health Organization. WHO calls for safe and ethical AI for health. Geneva: World Health Organization; 2023 May 16.
3. World Health Organization. Artificial intelligence and evidence-informed policy—emerging challenges and

- opportunities. Geneva: World Health Organization; 2026 Jun 2.
4. IEEE Author Center Conferences. Structure your paper [Internet]. IEEE; 2026.
 5. National Institute of Standards and Technology. *Artificial intelligence risk management framework (AI RMF 1.0)*. Gaithersburg (MD): National Institute of Standards and Technology; 2023.

Creative Commons License

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution–Non-commercial–No Derivatives 4.0 International (CC BY-NC-ND 4.0) License. This license permits users to copy and redistribute the material in any medium or format for non-commercial purposes only, provided that appropriate credit is given to the original author(s) and the source. No modifications, adaptations, or derivative works are permitted.

About the Author



Vaibhav Bhosle is affiliated with the Department of Science and Technology at Shivaji University, Kolhapur, India. His academic interests focus on science and technology, with an emphasis on research and scholarly activities. He contributes to the academic environment through research, learning, and engagement in scientific and technological developments.