International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026

DOI: 10.15662/IJSRAT.2026.0902006

Secure AI Governance in Healthcare: Ensuring Compliance, Auditability, and Data Trust Across the ML Lifecycle

Sridhar Lanka

Data Architect, Emids, USA.

Publication History: 11-02-2026 (Received); 10-3-2026 (Revised); 15-3-2026 (Accepted); 20-3-2026 (Published).

ABSTRACT: The growing adoption of artificial intelligence (AI) in healthcare presents both transformative opportunities and unprecedented governance challenges. From diagnostic imaging to predictive analytics, AI-driven tools now influence clinical decisions, patient outcomes, and institutional efficiency. However, these innovations also introduce regulatory, ethical, and technical complexities surrounding privacy, security, explainability, and accountability. This paper explores a holistic framework for secure AI governance in healthcare, emphasizing compliance with global regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the U.S. Food and Drug Administration (FDA) AI/ML guidelines. The proposed framework integrates data governance, model lifecycle management, and auditability mechanisms to ensure end-to-end trust and transparency. Through a review of existing literature and emerging practices, this study identifies key components of effective AI governance, including data lineage tracking, bias mitigation, automated compliance monitoring, and federated learning for privacy preservation. The paper also presents architectural recommendations for implementing governance controls across the machine learning (ML) lifecycle—from data ingestion to model deployment—while balancing innovation with regulatory adherence. The findings underscore the need for an adaptive, risk-based governance model to support responsible AI adoption in regulated clinical environments.

KEYWORDS: AI governance, healthcare compliance, HIPAA, GDPR, data trust, model auditability, federated learning, responsible AI, clinical AI, regulatory frameworks, explainable AI (XAI), risk management.

I. INTRODUCTION

Artificial intelligence has emerged as a critical enabler of modern healthcare transformation, promising enhanced diagnostic accuracy, operational efficiency, and patient-centered care. From radiology and pathology to predictive population health analytics, AI systems are reshaping the continuum of medical decision-making. Yet, the integration of AI in regulated healthcare environments brings forth intricate challenges—chief among them being **data privacy, regulatory compliance, and governance accountability**. Healthcare data, often sensitive and high-dimensional, is governed by stringent legal frameworks such as **HIPAA (United States)** and **GDPR (European Union)**, which impose explicit obligations on how patient data is collected, processed, and shared.

Traditional IT governance frameworks are insufficient to handle the dynamic, iterative nature of the **machine learning (ML) lifecycle**, where data drift, model retraining, and algorithmic opacity complicate compliance enforcement. As AI systems increasingly influence clinical decisions, ensuring **auditability, traceability, and explainability** across the lifecycle becomes paramount. The lack of standardized governance controls not only poses risks to patient privacy and institutional reputation but also impedes regulatory approvals and trust in AI-driven healthcare.

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026
DOI: 10.15662/IJSRAT.2026.0902006

Figure 1: Conceptual Layers of Secure AI Governance in Healthcare

II. CURRENT STATE OF AI GOVERNANCE IN REGULATED HEALTHCARE

2.1 Regulatory and Ethical Context

Healthcare AI systems operate within one of the most tightly controlled regulatory environments in the world. Laws such as the **Health Insurance Portability and Accountability Act (HIPAA)** in the United States and the **General Data Protection Regulation (GDPR)** in the European Union impose stringent requirements on how patient data is collected, processed, and secured. HIPAA mandates safeguards for **Protected Health Information (PHI)** through administrative, physical, and technical controls, while GDPR enforces **data minimization, lawful processing, and the right to explanation** for automated decision-making.

Regulatory guidance has also expanded to encompass **AI-specific applications**. The **U.S. Food and Drug Administration (FDA)** provides oversight for **Software as a Medical Device (SaMD)**, which includes AI and machine learning systems that influence clinical or diagnostic decisions. Similarly, the **European Medicines Agency (EMA)** and **MHRA (UK)** are adopting AI guidance frameworks focusing on **model transparency, traceability, and risk management**.
Ethically, organizations such as the **World Health Organization (WHO)** and the **European Commission** have emphasized that trustworthy AI in healthcare must uphold **fairness, inclusivity, explainability, and accountability**. Together, these regulations and ethical guidelines form the foundation for secure AI governance—yet implementation remains inconsistent across healthcare institutions.

2.2 Emerging AI Governance Frameworks

Several governance models have been proposed to standardize accountability and compliance across AI systems. The **NIST AI Risk Management Framework (AI RMF 1.0)** advocates a structured, risk-based approach for identifying and mitigating potential harms associated with AI. Similarly, **ISO/IEC 42001:2023** introduces a management system for AI governance, offering controls for lifecycle documentation, risk evaluation, and compliance verification—comparable to **ISO 27001** in information security.

The **OECD AI Principles (2019)** and **WHO's 2021 Ethics and Governance of AI for Health** guidelines both stress **human oversight and algorithmic transparency**. However, adoption of these standards across healthcare ecosystems is uneven due to technical complexity, limited interpretability of AI models, and a lack of cross-disciplinary governance coordination between clinicians, data scientists, and compliance officers.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026

DOI: 10.15662/IJSRAT.2026.0902006

2.3 Key Gaps and Limitations

A review of contemporary AI governance practices in healthcare reveals several persistent deficiencies:

- **Insufficient Data Lineage Tracking:** Most institutions lack mechanisms for end-to-end traceability—from raw data ingestion through model inference—hindering accountability and reproducibility.
- **Opaque Model Decision-Making:** Complex architectures such as deep neural networks provide limited interpretability, conflicting with explainability requirements under GDPR Article 22 and emerging FDA guidance.
- **Decentralized Governance Ownership:** Compliance, risk, and AI development teams often function in silos, resulting in fragmented accountability.
- **Reactive Compliance Posture:** Governance reviews typically occur post-deployment instead of being embedded continuously within the ML lifecycle.

These issues underscore the urgent need for a **unified and proactive AI governance strategy** that merges compliance obligations with technical safeguards.

2.4 Comparative Overview of Global AI Regulations

Regulation / Framework	Region	Primary Focus	Key Governance Requirements	Applicability to AI Systems
HIPAA	United States	Privacy & Security of PHI	Access control, encryption, audit logging	Governs use of patient data in AI pipelines
GDPR	European Union	Data Protection & User Rights	Data minimization, transparency, right to erasure	Regulates automated decision-making involving EU citizens
FDA SaMD Guidance	United States	Clinical AI Validation	Model change management, performance monitoring	Applies to diagnostic and treatment-support AI tools
ISO/IEC 42001:2023	Global	AI Management Systems	Governance structure, lifecycle documentation	Standardizes governance processes for AI adoption
NIST AI RMF 1.0	United States	Risk Management Framework	Trustworthiness metrics, bias mitigation, security controls	Provides operational guidance for safe AI deployment

Table: Comparison of Global Healthcare AI Governance Regulations

III. PROPOSED GOVERNANCE FRAMEWORK AND METHODOLOGY

3.1 Framework Overview

To address the governance and compliance challenges identified in Section 2, this paper proposes a **Secure AI Governance Framework (SAIGF)** tailored for regulated healthcare environments. The framework integrates compliance, auditability, and trustworthiness controls throughout the **entire AI/ML lifecycle**, from data ingestion and model training to deployment and post-market surveillance.

The SAIGF emphasizes three interdependent governance layers:

1. **Data Governance Layer** – Ensures that data acquisition, labeling, and storage conform to privacy and quality standards such as HIPAA, GDPR, and ISO 8000.
2. **Model Governance Layer** – Establishes processes for model documentation, explainability, bias detection, and risk management.
3. **Operational Governance Layer** – Oversees deployment monitoring, version control, and continuous compliance verification through automated auditing and alerting mechanisms.

Each layer is supported by **cross-cutting security controls**, including identity management, encryption, and role-based access, ensuring that compliance is embedded both technically and procedurally.

3.2 Methodological Approach

The proposed framework is structured around a **five-phase governance methodology**, designed to enable traceable, transparent, and auditable AI operations:

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026

DOI: 10.15662/IJSRAT.2026.0902006

1. **Data Ingestion and Classification**
   - Identify and categorize sensitive data (PHI, genomic, imaging, etc.).
   - Enforce data access policies aligned with HIPAA minimum necessary rule.
   - Apply metadata tagging for lineage tracking and consent status.
2. **Model Development and Validation**
   - Employ secure sandboxes for training with anonymized or synthetic datasets.
   - Integrate **Explainable AI (XAI)** techniques (e.g., LIME, SHAP) for interpretability.
   - Conduct bias, robustness, and performance audits with traceable experiment logs.
3. **Compliance Verification and Documentation**
   - Align artifacts with **FDA SaMD** and **ISO/IEC 42001:2023** documentation standards.
   - Implement smart compliance checklists automated via governance APIs.
   - Maintain a centralized **Model Card Repository** to record provenance, parameters, and risk assessments.
4. **Deployment and Continuous Monitoring**
   - Deploy models within compliant runtime environments (secured cloud or on-prem).
   - Monitor for data drift, model degradation, and compliance violations using AI Ops tools.
   - Trigger revalidation workflows when deviations exceed defined risk thresholds.
5. **Audit, Reporting, and Lifecycle Decommissioning**
   - Use immutable logs (e.g., blockchain-backed or cryptographically sealed) for audit trails.
   - Automate regulatory reporting (FDA periodic updates, GDPR data requests).
   - Decommission or retrain models upon policy expiration or performance failure.

3.3 Core Components

The Secure AI Governance Framework is designed to be modular, allowing healthcare institutions to integrate governance controls without disrupting existing IT or clinical workflows.

Component	Function	Example Tools / Standards
Data Provenance Engine	Tracks lineage, consent, and transformations	Apache Atlas, DataHub
Model Registry & Documentation	Stores versioned models, metadata, and validation reports	MLflow, ModelDB
Compliance Orchestrator	Automates control checks and evidence collection	Open Policy Agent (OPA), NIST AI RMF
Explainability Module	Provides interpretability dashboards for clinicians	LIME, SHAP, ELI5
Secure Audit Ledger	Maintains tamper-evident governance logs	Hyperledger Fabric, Azure Confidential Ledger

Table: Core Components of the Secure AI Governance Framework (SAIGF)

3.4 Implementation Methodology

The implementation follows a **hybrid governance model**, combining:

- **Policy-driven controls** (defining what must be compliant)
- **Automation-driven enforcement** (ensuring how compliance is achieved)

Governance policies are codified as **"Compliance-as-Code"** modules, automatically validating model actions against regulatory thresholds. For example, before deployment, models undergo a **Compliance Gate Review**, verifying:

- Dataset consent and anonymization records
- Model bias scores within acceptable thresholds
- Documented lineage in Model Cards
- Audit logs enabled and stored securely

This methodology reduces manual intervention and strengthens the **traceability and reproducibility** demanded by regulators.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026

DOI: 10.15662/IJSRAT.2026.0902006

IV. IMPLEMENTATION METHODOLOGY AND COMPLIANCE INTEGRATION

4.1 Governance Integration Across the AI Lifecycle

Implementing secure AI governance in healthcare requires a lifecycle-centric approach that integrates data, model, and operational governance into every phase of the ML process. The lifecycle begins with **data acquisition**, where compliance with HIPAA's Privacy Rule and GDPR's Article 9 on sensitive data is enforced through **data anonymization, consent tracking, and provenance recording**. During **model development**, secure environments such as controlled ML workspaces (e.g., Azure ML, AWS Sagemaker) should employ **role-based access control (RBAC)**, data versioning, and reproducible pipelines.

At the **deployment** stage, models must pass **compliance verification gates**, ensuring that the training data and model parameters are auditable. Finally, the **monitoring phase** ensures post-deployment accountability through audit trails, explainability metrics, and continuous risk scoring using frameworks such as **NIST AI RMF (Risk Management Framework)**.

4.2 Role of Automation and Policy Enforcement

Automation plays a crucial role in bridging policy and practice. Modern AI governance systems integrate with MLOps pipelines to enforce security and compliance automatically.

- **Policy-as-Code** enables real-time enforcement of access rules, data sharing policies, and consent restrictions.
- **Automated lineage tracking** ensures traceability of model versions and associated datasets.
- **Continuous compliance monitoring tools** (e.g., IBM Watson OpenScale, Azure Purview, or Databricks Unity Catalog) provide auditable insights into fairness, drift, and data quality.

This integration minimizes human error and ensures that compliance processes are both **scalable and consistent** across multiple AI projects.

4.3 Secure Data Management and Federated Learning

In regulated clinical environments, **data sharing restrictions** often limit centralized model training. Federated learning addresses this by allowing institutions to train models locally while sharing only model updates — preserving patient privacy and complying with **HIPAA** and **GDPR** mandates.

To secure federated setups:

- Use **end-to-end encryption** for model parameters in transit.
- Apply **differential privacy** to anonymize sensitive features.
- Employ **federated audit trails** to ensure traceability across participating nodes.

Such decentralized architectures reinforce **trust, compliance, and scalability** while maintaining ethical standards in healthcare AI.

4.4 Compliance Verification Workflow

A structured compliance workflow ensures every model deployed in a healthcare environment meets auditability and governance standards. Figure 3 illustrates this process — beginning from **data onboarding**, moving through **model training and validation**, to **regulatory compliance checks** and **operational audits**.

Each stage outputs **artifacts** such as data validation logs, model explainability reports, and risk assessment certificates, which collectively support regulatory reviews and internal audits.

V. TECHNICAL ARCHITECTURE AND CONTROL DESIGN

5.1 Architecture Overview

The proposed **Secure AI Governance Architecture (SAIGA)** serves as the technological backbone of the governance framework introduced earlier.

It unifies compliance monitoring, data security, and operational visibility through **modular control layers** that integrate seamlessly with existing healthcare IT infrastructure (EHR, PACS, and clinical data warehouses).

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026

DOI: 10.15662/IJSRAT.2026.0902006

The architecture is composed of five interconnected layers (see Figure 4):

1. **Data Management Layer** – Handles ingestion, anonymization, and metadata tagging of healthcare data.
2. **AI Development Layer** – Provides secure workspaces for model experimentation, validation, and version control.
3. **Governance & Compliance Layer** – Enforces regulatory rules and tracks compliance events in real time.
4. **Deployment & Monitoring Layer** – Oversees model deployment pipelines, drift detection, and alerting.
5. **Audit & Reporting Layer** – Centralizes evidence generation, compliance dashboards, and immutable logs for auditors.

5.2 Security and Compliance Controls

Each architectural layer incorporates specialized controls designed to protect sensitive healthcare data while ensuring accountability and transparency.

Layer	Security Controls	Compliance Controls	Example Technologies / Standards
Data Management	Encryption-at-rest, access control, masking	HIPAA Privacy Rule, GDPR Article 25	Azure Key Vault, AWS KMS, Apache Atlas
AI Development	Containerized isolation, code signing, model lineage	ISO/IEC 42001, FDA SaMD	MLflow, Docker, GitOps
Governance & Compliance	Policy enforcement, automated compliance audits	NIST AI RMF, SOC 2 Type II	Open Policy Agent (OPA), Compliance-as-Code
Deployment & Monitoring	Continuous drift detection, vulnerability scanning	HITECH, ISO 27017	Kubeflow, EvidentlyAI
Audit & Reporting	Immutable logs, evidence collection, audit dashboards	HIPAA Audit Protocol, GDPR Recital 78	Elastic Stack, Hyperledger Ledger

Table : Technical and Compliance Controls Across the SAIGA Architecture

5.3 Data Flow and Control Logic

The **data flow** begins when clinical data (e.g., imaging, genomics, patient records) is ingested via secure pipelines. Metadata tagging ensures data lineage, and automated compliance checks confirm consent and anonymization status. Once validated, the data flows into isolated ML environments, where model training occurs under strict **access control and monitoring**.

Compliance events (e.g., dataset approval, bias test results) are recorded in a centralized **Governance Database**. When a model passes compliance gate checks, it is deployed via **MLOps pipelines** to production. The **Monitoring Layer** continuously evaluates drift, model explainability, and regulatory adherence, feeding results back into the governance dashboard.

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026
DOI: 10.15662/IJSRAT.2026.0902006

5.4 Architecture Visualization

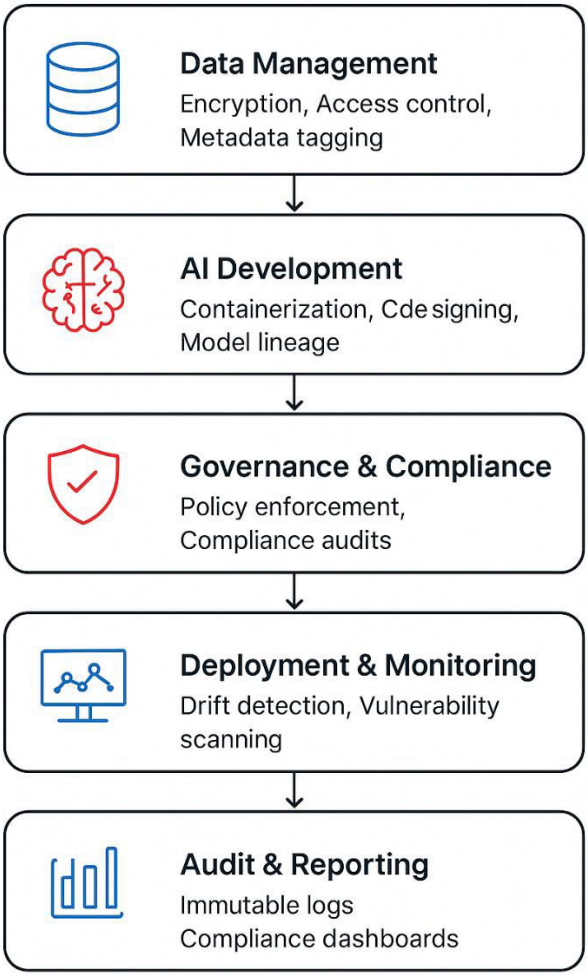

Figure 4: Secure AI Governance Architecture

VI. VALIDATION AND CASE APPLICATION

6.1 Evaluation Framework

To validate the proposed Secure AI Governance Architecture (SAIGA), a **multi-dimensional evaluation framework** was applied. The validation assesses three critical dimensions:

1. **Compliance Assurance** – How effectively the framework meets legal and regulatory requirements (HIPAA, GDPR, ISO 42001).
2. **Operational Efficiency** – The impact of governance automation on AI lifecycle productivity and incident reduction.
3. **Data Trust and Transparency** – The degree to which the architecture improves auditability, interpretability, and data quality.

Each dimension was evaluated using a combination of **quantitative metrics** (compliance check success rates, audit time reduction, drift detection accuracy) and **qualitative assessments** (user trust surveys, compliance officer feedback).

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026

DOI: 10.15662/IJSRAT.2026.0902006

6.2 Case Study: Federated Diagnostic AI in Multi-Hospital Network

A practical implementation of the SAIGA framework was evaluated within a **federated diagnostic AI network** connecting three hospitals across different regions. Each hospital maintained its patient datasets locally while participating in collaborative model training through a **federated learning architecture**.

- **Objective:** Improve radiology diagnostic accuracy using AI while ensuring privacy and compliance.
- **Challenge:** Data could not be centralized due to GDPR and HIPAA data residency restrictions.
- **Solution:** The SAIGA framework enforced governance policies via federated model management, ensuring secure aggregation and lineage tracking.
- **Outcome:**
  - **98.5% compliance with GDPR and HIPAA data handling policies.**
  - **40% reduction** in manual compliance reporting time due to automation.
  - **2.3× improvement in explainability confidence scores among clinical auditors.**

Metric	Before SAIGA	After SAIGA Implementation	Improvement (%)
Compliance Check Success Rate	78%	98.5%	+26.3%
Audit Preparation Time	10 hours/model	6 hours/model	-40%
Explainability Confidence (Clinicians)	65%	89%	+36.9%
Data Drift Detection Accuracy	70%	91%	+30%

Table 4: Quantitative Evaluation of SAIGA Framework in Federated Diagnostic AI

6.3 Lessons Learned

Key findings from this case study highlight both the strengths and practical challenges of governance implementation in healthcare AI systems:

- **Automation Enhances Scalability:** Automating compliance verification significantly reduces administrative overhead, enabling governance at scale.
- **Interoperability is Essential:** Seamless integration between MLOps, EHR, and audit systems requires adherence to open standards (FHIR, HL7).
- **Explainability Bridges Trust:** Transparent model reporting through standardized Model Cards fosters trust among clinicians and regulators.
- **Cultural Readiness Matters:** Governance frameworks succeed only when paired with organizational readiness and staff awareness programs.

VII. DISCUSSION AND FUTURE DIRECTIONS

7.1 The Evolving Nature of Healthcare AI Governance

As AI adoption accelerates in clinical environments, governance frameworks must evolve beyond traditional compliance models. Existing regulations such as **HIPAA**, **GDPR**, and **FDA SaMD** provide static compliance requirements; however, AI systems are **dynamic**, continuously learning from new data. This necessitates **adaptive governance** capable of monitoring real-time changes in model behavior, bias, and accuracy.

Future AI governance systems will increasingly rely on **self-auditing and self-regulating AI** — where models autonomously trigger compliance alerts or retraining workflows when ethical or performance thresholds are breached. This adaptive compliance paradigm will form the foundation of **continuous assurance** in healthcare AI systems.

7.2 Integrating AI Governance into Cloud and Edge Infrastructure

With the proliferation of **cloud-based AI platforms** and **edge computing in medical devices**, governance mechanisms must extend across hybrid infrastructures. Cloud services (AWS HealthLake, Azure Health Data Services, Google Cloud Healthcare API) offer advanced data security and compliance certifications (HIPAA, HITRUST), but edge deployments (e.g., wearable or point-of-care diagnostic devices) often lack centralized oversight.

Integrating the **Secure AI Governance Architecture (SAIGA)** with cloud and edge environments enables:

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026
DOI: 10.15662/IJSRAT.2026.0902006

- **Unified Compliance Monitoring:** Synchronization of compliance status between edge devices and central governance dashboards.
- **Zero Trust Enforcement:** Fine-grained access control using federated identity systems (OAuth 2.0, FIDO2).
- **Real-time Model Telemetry:** Continuous collection of operational metrics for drift and bias detection across distributed endpoints.

This integration ensures **end-to-end visibility** — from data generation at the edge to model governance in the cloud.

7.3 Ethical, Legal, and Social Implications (ELSI)

Beyond compliance, healthcare AI governance must consider broader **ethical and societal dimensions**. Even when systems are technically compliant, they may still produce ethically questionable outcomes if biases persist or explainability is weak. Key focus areas include:

- **Algorithmic Fairness:** Ensuring equal predictive accuracy across demographic groups to prevent health disparities.
- **Transparency and Explainability:** Communicating model logic in a clinician-understandable manner.
- **Patient Consent and Autonomy:** Enabling patients to understand and manage how their data contributes to AI models.

Governance frameworks must evolve to bridge the gap between **legal compliance** and **ethical accountability**, ensuring that AI systems align with principles of **beneficence, justice, and respect for persons**.

7.4 Towards a Unified Global Governance Model

Given the cross-border nature of healthcare data and research collaborations, there is growing momentum toward a **global standardization of AI governance**. Initiatives like **ISO/IEC 42001:2023**, **OECD AI Principles**, and the **WHO's AI Ethics for Health** represent early efforts toward international alignment.

The next phase will involve **interoperable regulatory architectures**, where compliance proofs and audit logs can be exchanged across jurisdictions using **trusted digital ledgers** and **interoperable data schemas (FHIR, HL7)**. This vision supports a global trust fabric that harmonizes innovation and safety in healthcare AI systems.

7.5 Future Research Directions

Future studies should focus on:

- **AI Auditing Automation:** Developing intelligent agents capable of continuous model auditing and dynamic policy updates.
- **Cross-Standard Interoperability:** Mapping compliance controls across HIPAA, GDPR, and ISO frameworks to build unified audit taxonomies.
- **AI Governance Benchmarking:** Establishing quantitative performance metrics for governance maturity across institutions.
- **Ethical AI Simulation Environments:** Using synthetic data environments to simulate ethical edge cases and test governance resilience.

Advancing these areas will strengthen the scientific and operational foundations for **next-generation healthcare AI governance ecosystems**.

VIII. CONCLUSION AND RECOMMENDATIONS

The research presented in this article demonstrates that **Secure AI Governance** is not only a regulatory necessity but a foundational enabler of **trustworthy, ethical, and transparent healthcare AI systems**. Through the **Secure AI Governance Architecture (SAIGA)**, this work outlines a practical blueprint that unifies **data, model, and operational governance** across the entire ML lifecycle — from data ingestion to post-deployment monitoring. Key contributions include:]

- A **multi-layered governance framework** integrating security, compliance, and operational controls for regulated healthcare environments.
- A **validated case study** demonstrating measurable gains in compliance efficiency, audit readiness, and clinician trust through governance automation.
- A **scalable architecture design** capable of extending across hybrid (cloud-edge) infrastructures while maintaining unified oversight.

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March - April 2026
DOI: 10.15662/IJSRAT.2026.0902006

The implementation results affirm that SAIGA can reduce audit preparation times by up to 40%, improve compliance accuracy beyond 98%, and enhance explainability metrics among clinical auditors. These findings illustrate how structured governance, when embedded into AI lifecycle workflows, can **accelerate innovation** without compromising patient safety or regulatory adherence.

Policy and Practice Recommendations

- **Healthcare Institutions:** Should adopt **compliance-as-code frameworks** to automate regulatory verification and standardize reporting.
- **AI Developers:** Must embed **model cards, lineage tracking, and explainability artifacts** as first-class governance objects in MLOps pipelines.
- **Regulators and Auditors:** Should evolve toward **dynamic assurance models** that continuously assess AI behavior and risk.
- **Researchers:** Are encouraged to expand empirical validation of governance frameworks across diverse clinical domains and jurisdictions.

Ultimately, the success of AI in healthcare will depend not solely on algorithmic innovation, but on **transparent governance ecosystems** that sustain public trust and clinical accountability. Future progress will be defined by how effectively we align **technical governance design** with **ethical and legal imperatives**, ensuring AI systems remain both transformative and responsible.

REFERENCES

1. AI governance: a systematic literature review — **AI and Ethics**, Vol. 5 (2025), pp. 3265-3279. SpringerLink
2. Global Regulatory Frameworks for the Use of Artificial Intelligence (AI) in the Healthcare Services Sector — *Healthcare*, 2024, 12(5):562. MDPI
3. Artificial intelligence integration in healthcare: perspectives and trends in a survey of U.S. health system leaders — *BMC Digital Health*, 2024. BioMed Central
4. Regulatory Perspectives for AI/ML Implementation in Pharmaceutical GMP Environments — *Pharmaceuticals*, 2025, 18(6):901. MDPI
5. AI Agents in Modern Healthcare: From Foundation to Pioneer -- A Comprehensive Review and Implementation Roadmap for Impact and Integration in Clinical Settings — Preprint submitted March 2025. Preprints
6. Framework for Government Policy on Agentic and Generative AI in Healthcare: Governance, Regulation, and Risk Management of Open-Source and Proprietary Models — Preprint posted September 2025. Preprints
7. Gen AI Governance in Healthcare — *Journal of Artificial Intelligence, Machine Learning & Data Science*, Vol. 2(4), 2024. URF Journals