



Policy Brief

AI Risk Management Framework for the Healthcare Sector (Systems and Services)

Track 2: Deployment & Application Regulation

Prepared by:
Maria T Mansoor
Vibhuti Dahiya

Executive Summary

AI Risk Management Framework for the Healthcare Sector

Background	- AI is revolutionizing healthcare through enhanced clinical decision-making, operational efficiency, and patient engagement. - Challenges include data privacy, algorithmic bias, and lack of transparency in AI systems.
Current Regulatory Landscape	- Federal laws addressing healthcare AI remain stalled; state-level regulations (e.g., California SB 1120, AB 3030) provide fragmented oversight. - Need for a unified, open-source framework to democratize access and ensure compliance across all healthcare organizations.
Proposed Solution: Comprehensive AI Risk Management Framework	- Governance & Oversight: Establish accountability and ethical alignment. - Identification: Map AI systems, data flows, and risks. - Alignment: Ensure regulatory and stakeholder compliance. - Management: Implement robust risk controls and monitoring. - Continuous Improvement: Evaluate performance and drive iterative enhancements.
Call to Action	The Department of Health and Human Services (HHS) should lead the development of an open-source framework to address AI-specific challenges while ensuring compliance with HIPAA and HITECH regulations.
Key Benefits	- Improved patient safety and trust. - Enhanced operational efficiency. - Equitable access to AI governance tools for all healthcare institutions.

Background

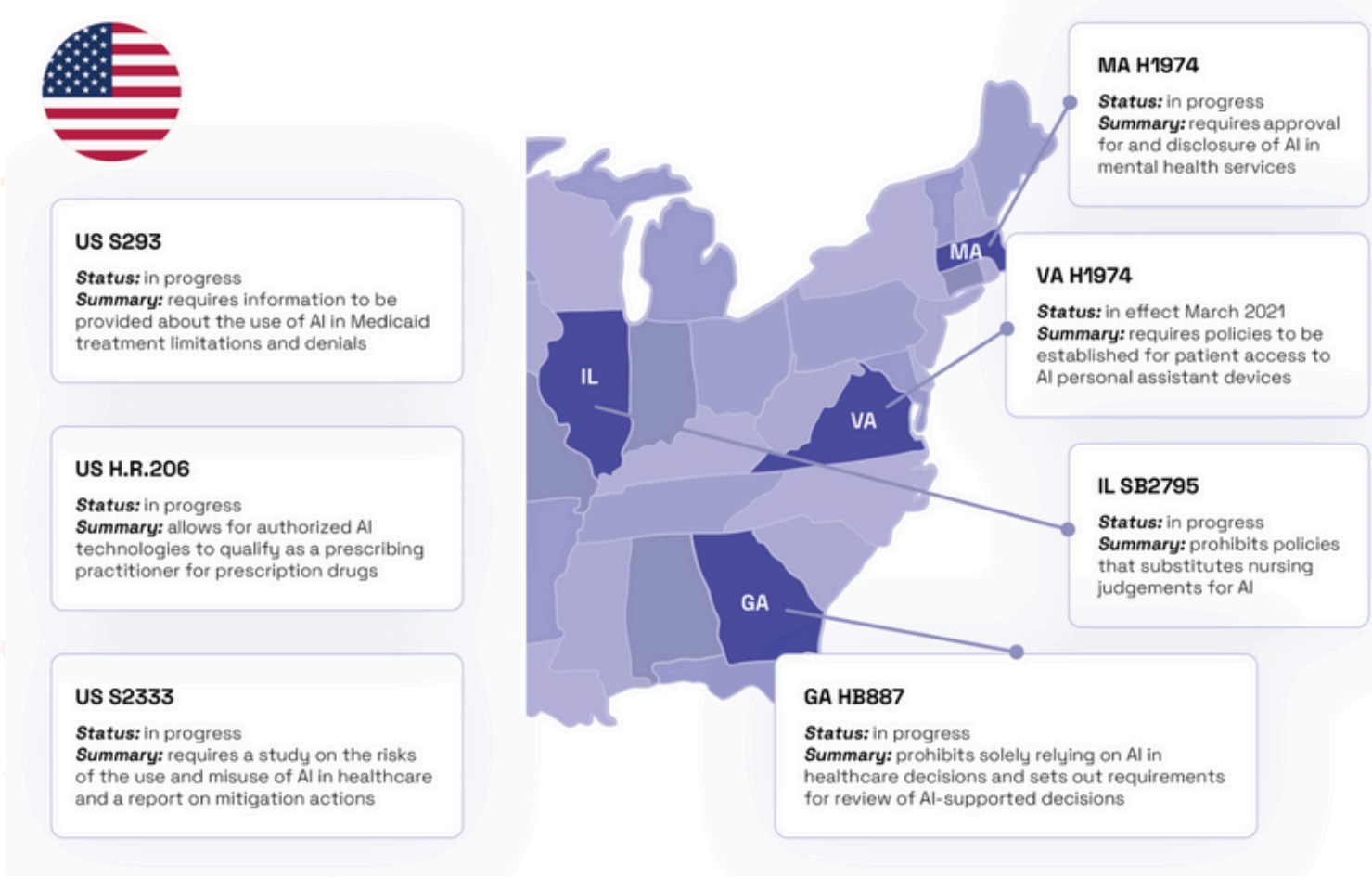
Current Situation: Addressing the Lack of a Standard Framework for AI in Healthcare

Growing Role of AI in Healthcare	Clinical Decision Support	AI systems analyze patient data to diagnose and treat, enhancing decision-making accuracy and efficiency (Ferrara, et al., 2024; Ranjbar, et al., 2024).
	Operational Efficiency	Predictive analytics optimize hospital operations such as staffing, supply chain management, and billing processes (HITRUST, 2023)
	Patient Engagement	AI-powered chatbots and personalized care applications improve communication between patients and providers, fostering adherence to treatment plans and overall satisfaction (Palaniappan, Lin, & Vogel, 2024).

Challenges with AI in Healthcare

Data Privacy and Security	AI systems require large datasets, raising concerns about how Protected Health Information (PHI) is collected, stored, and used. Current regulations like HIPAA do not sufficiently address the unique challenges posed by AI, such as securing training data or preventing unauthorized access (HITRUST, 2023; Palaniappan, Lin, & Vogel, 2024).
Algorithmic Bias	Without proper oversight, AI algorithms may perpetuate biases present in training data, leading to inequitable outcomes. For instance, FDA-approved medical devices have faced criticism for bias against underrepresented populations (Ferrara, et al., 2024; Palaniappan, Lin, & Vogel, 2024)
Transparency and Accountability	Many AI systems function as "black boxes," making it difficult to understand their decision-making processes or hold them accountable for errors. This lack of transparency undermines trust in AI-driven healthcare solutions (National Institute of Standards and Technology, 2023; HITRUST, 2023)

Current State of Healthcare AI Regulations in the US



The majority of laws in the US targeting AI in healthcare are still in the proposal stage at both the Federal and State levels.

Source:
Holistic AI

Background

Lack of Passed Federal Laws Targeting AI in Healthcare

Despite the growing need for regulation, many federal laws addressing AI in healthcare remain in the proposal stage and have yet to pass into law:

- The Better Mental Health Care for Americans Act (S293) proposes transparency requirements for mental health treatment decisions made using AI but has not progressed beyond initial discussions (Miller, 2025; Considering The Future Of AI Regulation On Health Sector, 2025).
- The Healthy Technology Act of 2025 (H.R.238) seeks to authorize FDA-approved AI systems as practitioners eligible to prescribe medications under certain conditions but remains under review (Healthy Technology Act of 2025: AI Prescribing Bill Introduced in Congress, 2025)
- Other bills addressing critical issues like bias mitigation, transparency, and accountability have similarly stalled at both federal and state levels (Considering The Future Of AI Regulation On Health Sector, 2025; Hilliard, 2024)
- While federal action has been limited, states have introduced numerous bills targeting the use of AI in healthcare—629 bills across 46 states were tracked in 2025 alone (Miller, 2025). However, only a small fraction of these bills have been enacted into law, with most failing to pass or being reintroduced in revised forms later (Hilliard, 2024; Miller, 2025).

Current State of Healthcare AI Regulations in the US

Legislature	Brief Description	Effective Date	Summary of Compliance Tasks
AB 3030	Health care AI communications require disclaimers and contact info.	January 1, 2025	Health care providers must supply disclaimers that indicate to patients that the communication was generated by gen AI intelligence.
SB 1120	Only physicians can independently decide medical necessity, not AI.	January 1, 2025	Denials, delays or modifications of health care services based on medical necessity must be made by a licensed physician or other competent health care provider. Ensure that AI-based determinations for health plans' prior authorization and management functions are reviewed and approved with adequate human oversight and not AI alone.

Source: Pillsbury

Two new California laws regulate the use of AI in connection with health care services, communicating, medical decisions, and protecting neural & biological data privacy.

Existing Solutions and Limitations

State-Specific Healthcare AI Laws

HITRUST's AI Assurance Program

California has implemented state-specific regulations (CA SB 1120 and CA AB 3030) (Serrato, et al., 2025) requiring disclosure when generative AI is used in clinical communications and compliance with utilization review requirements (Miller, 2025). Virginia has also enacted legislation (HB2154) requiring hospitals, nursing homes, and certified nursing facilities to establish policies governing the use of intelligent personal assistants powered by AI. However, these laws are not standardized across the country and benefit only Californian and Virginia institutions (Hilliard, 2024)

This program provides a governance framework for managing AI risks but is limited to HITRUST customers, restricting its accessibility to the broader healthcare sector (HITRUST, 2023; HITRUST, n.d.)

Need for an Open-Source Framework

- Current frameworks like HITRUST's are valuable but proprietary, creating barriers for smaller organizations that lack resources to access such tools. Similarly, state-level regulations like those in California are fragmented and fail to provide a unified approach to governing AI in healthcare (Considering The Future Of AI Regulation On Health Sector, 2025; Hagen & Vecchione, 2025).
- An open-source framework would democratize access to governance tools, enabling all healthcare organizations—regardless of size or location—to implement robust risk management practices for AI (Hilliard, 2024; Healthy Technology Act of 2025: AI Prescribing Bill Introduced in Congress, 2025)

Call to Action for the Department of Health and Human Services (HHS)

1.The Office for Civil Rights within HHS should lead the development of a comprehensive Risk Management Framework (RMF) tailored to the use of AI in healthcare. This framework should address critical areas such as:

- Ensuring compliance with existing regulations like HIPAA while adapting them to cover AI-specific challenges such as algorithmic transparency and secure handling of training data
- Promoting accountability through guidelines on ongoing auditing, system decommissioning, and lifecycle management of AI models (Hilliard, 2024; Considering The Future Of AI Regulation On Health Sector, 2025)
- Facilitating collaboration among stakeholders—including clinicians, technologists, ethicists, policymakers, and patient advocates—to create a governance model that balances innovation with patient safety and trust (Hagen & Vecchione, 2025)

Stakeholder Analysis			
Stakeholder	Roles & Responsibilities	Primary Concerns & Risks	Engagement & Strategies
Technology Companies	- Develop and market AI solutions for healthcare - Provide cloud and data management services	- High compliance burden, especially around HIPAA & HITECH - Liability for data breaches or algorithmic errors (U.S. Department of Health and Human Services Office for Civil Rights, 2013; The HIPAA Journal, n.d.) - Maintaining competitive advantage while meeting regulatory demands	- Establish Business Associate Agreements (BAA)to clarify shared responsibilities for ePHI (U.S. Department of Health and Human Services Office for Civil Rights, 2013; U.S. Department of Health and Human Services, 2009) - Participate in pilot programs to demonstrate compliance - Industry consortiums to standardize data formats, interoperability, and privacy measures
Healthcare Organizations (Public and Private)	- Deliver healthcare services, including treatment and prevention - Maintain secure and compliant electronic health record systems - Ensure regulatory compliance and manage procurement processes	- Cybersecurity threats, including data breaches and ransomware attacks (Healthcare-ISAC, 2025) - Outdated legacy systems hinder modernization and interoperability (Siwicki, 2025) - Complex regulations increase administrative and legal risks	- Upgrade legacy systems to interoperable, AI-compatible platforms (Venugopal, 2025) - Strengthen cybersecurity with encryption and multi-factor authentication - Create structured procurement guidelines emphasizing compliance standards
Individual Citizens	- Patients and healthcare consumers whose ePHI may be processed by AI - Family members involved in care decisions	- Fear of data misuse or breach (identity theft, discrimination) (U.S. Department of Health and Human Services Office for Civil Rights, 2013; The HIPAA Journal, n.d.) - Potential negative impact from biased or erroneous AI outputs (Accenture, 2022; Obermeyer, Powers, Vogeli, & Mullainathan, 2019) - Lack of clarity on data usage and sharing	- Provide transparent consent and data usage policies (easy-to-read privacy notices) - Develop patient feedback loops for AI-driven care (complaints, user experience, outcome tracking) - Encourage patient advocacy groups to participate in rule-making and audits
Academic Institutions	- Universities and research centers focusing on AI model development and clinical trials (Accenture, 2022; Obermeyer, Powers, Vogeli, & Mullainathan, 2019) - Often receive grants for advancing healthcare AI	- Complex IRB (Institutional Review Board) requirements for human subject research - Balancing open academic collaboration with privacy and intellectual property concerns - Ensuring data handling aligns with HIPAA & HITECH rules (Department of Health and Human Services Office for Civil Rights, 2013; U.S. Department of Health and Human Services, 2009)	- Adopt ethical and transparent research protocols(IRB, data use agreements) - Form joint research initiativeswith healthcare providers to test AI in real-world environments (Accenture, 2022) - Develop publicly accessible data libraries with privacy protections (e.g., de-identification)
International Partners	- Cross-border research collaborations - Multinational healthcare organizations or technology vendors - International regulatory bodies	- Differing legal frameworks (U.S. Department of Health and Human Services Office for Civil Rights, 2013; U.S. Department of Health and Human Services, 2009) - Complexity of cross-border data transfer and storage (The HIPAA Journal, n.d.) - Potential conflicts in data sovereignty and IP rights	- Develop international data-sharing protocolswith explicit consent and robust de-identification - Establish mutual recognition of AI certifications and audits to streamline compliance (U.S. Department of Health and Human Services Office for Civil Rights, 2013; U.S. Department of Health and Human Services, 2009) - Participate in global consortia for AI ethics and safety

AI Risk Management Framework for the Healthcare Sector (Systems and Services)

This framework is tailored to the healthcare sector with HIPAA & HITECH considerations, but restructured into five new functions reflecting defined goals. It integrates HIPAA & HITECH requirements and draws on key concepts from:

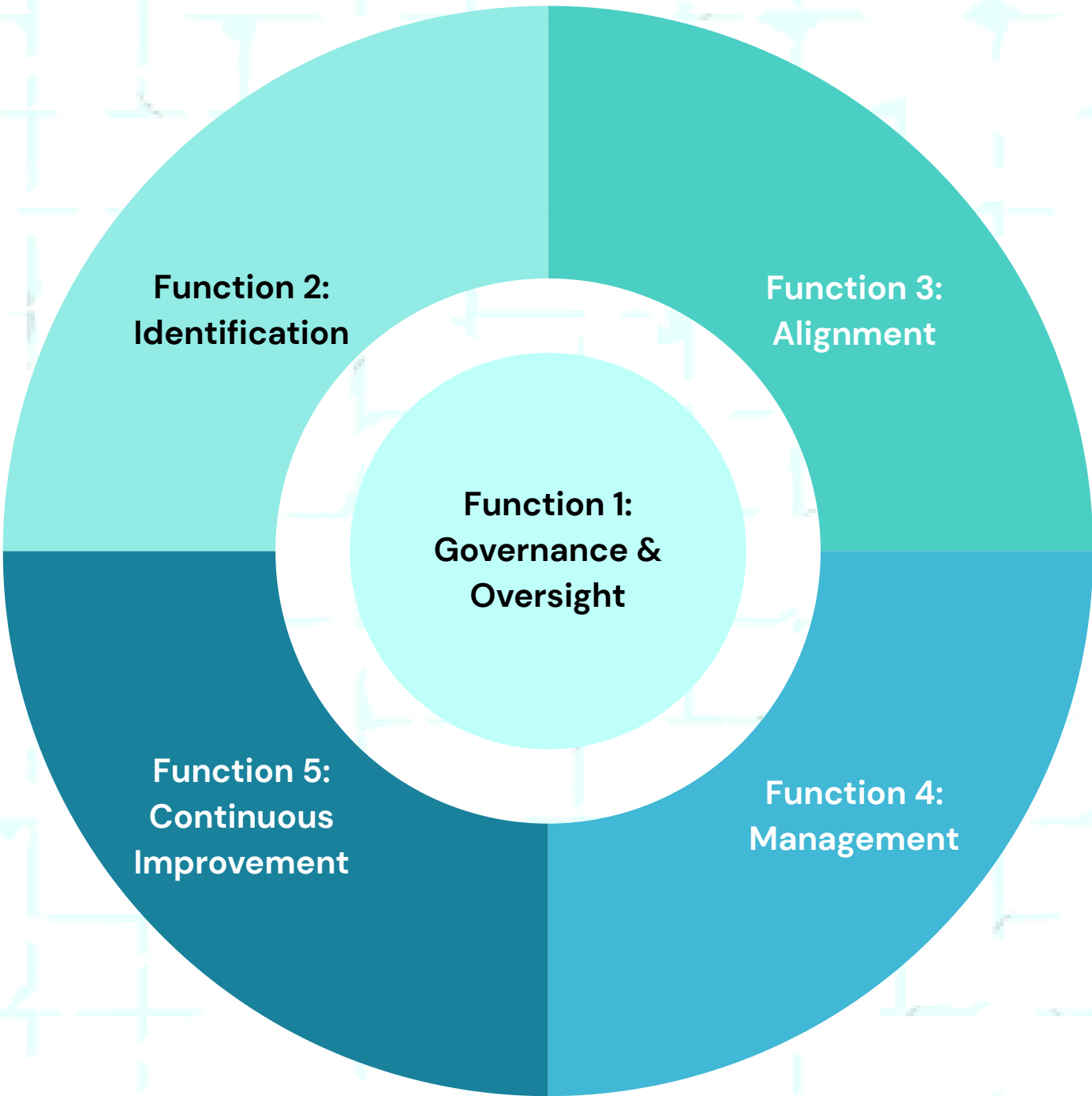
- NIST AI Risk Management Framework

NIST Privacy Framework
- NIST Cybersecurity Framework 2.0

ISO 42001:2023 Artificial Intelligence Management Systems

Each function includes healthcare-specific considerations for ePHI (electronic Protected Health Information), EHR (Electronic Health Records), and compliance obligations under HIPAA and HITECH.

Proposed AI Risk Management Framework
for the Healthcare Sector



Objectives of each Function of the Framework

Function 1: Governance & Oversight

Establish and maintain a clear organizational structure and decision-making authority for AI systems in healthcare, ensuring accountability, transparency, and alignment with ethical, legal, and regulatory requirements.

Function 2: Identification

Recognize, document, and understand all AI system components, data flows, and potential risks. This “Identification” phase sets the foundation for risk-informed decision-making throughout the AI lifecycle.

Function 3: Alignment

Align AI initiatives with organizational policies, regulatory requirements, and stakeholder expectations—then communicate these alignments effectively across all relevant parties.

Function 4: Management

Execute and maintain risk controls to manage identified AI risks effectively, ensuring continuous monitoring and prompt corrective action. This function also includes ongoing communication of risk posture and operational status.

Function 5: Continuous Improvement

Conduct both internal and external evaluations to verify compliance, assess AI performance and trustworthiness, and facilitate continuous improvement of AI governance in healthcare.

The Framework

Function 1: Governance & Oversight

Policy & Governance Board

- Form an **AI Governance Committee** composed of healthcare compliance officers, clinicians, data scientists, legal counsel, and patient advocacy representatives, aligned with guidance in (National Institute of Standards and Technology, 2023; National Institute of Standards and Technology, 2020).
- Define committee charters, meeting cadences, and escalation protocols for AI-related decisions.

Roles & Accountability

- Assign an **AI Compliance Officer** to ensure alignment with HIPAA & HITECH (U.S. Department of Health and Human Services Office for Civil Rights, 2013; U.S. Department of Health and Human Services, 2009) and track internal/external audits.
- Clearly delineate ownership of data sets, AI model lifecycle, and post-deployment monitoring.

Strategic Direction

- Set **organizational goals** for AI adoption (e.g., improved patient outcomes, operational efficiency, cost reduction) within a risk-informed framework [5].
- Incorporate **ethical principles** – fairness, transparency, and privacy protection – into policy documents (International Organization for Standardization, 2023).

Resource Allocation

- Allocate **budget** for robust security measures, staff training, and third-party risk assessments, consistent with (National Institute of Standards and Technology, 2024).
- Invest in **technology infrastructure** to support HIPAA-compliant data processing and secure AI model deployment (U.S. Department of Health and Human Services Office for Civil Rights, 2013).

Function 2: Identification

Asset and Data Mapping

- Catalog **all data sources** (EHR systems, lab results, imaging data) used for AI training, validation, and real-time inference.
- Create **data flow diagrams** showing how ePHI is collected, transformed, stored, and shared (International Organization for Standardization, 2023; U.S. Department of Health and Human Services Office for Civil Rights, 2013)

Risk Discovery

- Identify **potential vulnerabilities** related to data privacy (e.g., unauthorized access, insufficient de-identification) and AI integrity (model tampering, biased data).
- Classify AI use cases by **risk level** per (National Institute of Standards and Technology, 2023; National Institute of Standards and Technology, 2020; National Institute of Standards and Technology, 2024)

Stakeholder Mapping

- Pinpoint **internal stakeholders** (clinicians, IT, compliance teams) and **external stakeholders** (patients, vendors, regulators) with roles in data handling and AI deployment.
- Document each stakeholder’s data access level, compliance obligations, and potential impact on risk (National Institute of Standards and Technology, 2024).

Regulatory Requirements Check

- Review **HIPAA’s** “minimum necessary” standard (The HIPAA Journal, n.d.)in the context of each AI use case; confirm that only essential ePHI is used.
- Align with **HITECH** guidelines (U.S. Department of Health and Human Services, 2009) for EHR adoption, especially regarding secure data exchange and breach notification.

The Framework

Function 3: Alignment

Regulatory & Ethical Alignment

- Ensure AI systems adhere to **HIPAA & HITECH** privacy/security rules (U.S. Department of Health and Human Services Office for Civil Rights, 2013; U.S. Department of Health and Human Services, 2009), relevant state laws, and potential international frameworks.
- Integrate **ethical guidelines** into standard operating procedures (National Institute of Standards and Technology, 2024).

Organizational Coordination

- Align **executive leadership**, compliance teams, and clinical staff on AI implementation goals.
- Facilitate **cross-department collaboration** to avoid silos (IT, Legal, Medical, etc.) (National Institute of Standards and Technology, 2024).

Internal and External Communication

- **Internal:** Provide clear training and periodic updates to staff on AI tools, data usage, and compliance responsibilities (International Organization for Standardization, 2023).
- **External:** Proactively inform patients and partners about AI usage (e.g., disclaimers in patient portals, public statements on data governance).

Standards & Guidelines

- Adopt industry standards (e.g., ISO/IEC 27001 for information security) that complement healthcare regulations (The HIPAA Journal, n.d.).
- Collaborate with **professional associations** (e.g., AMA, HIMSS) to align on best practices and emerging standards for AI in healthcare (National Institute of Standards and Technology, 2024).

Function 4: Management

Risk Mitigation & Control Implementation

- Deploy **technical safeguards**: data encryption, access controls, intrusion detection, and continuous monitoring for anomalies.
- Implement **organizational measures**: staff training, strict onboarding/offboarding protocols, and vendor oversight (BAAs) (U.S. Department of Health and Human Services Office for Civil Rights, 2013).

Incident Response & Remediation

- Maintain a **HIPAA-compliant breach notification process** (60-day rule) and internal escalation pathways (U.S. Department of Health and Human Services Office for Civil Rights, 2013).
- Perform **root cause analysis** for AI performance issues or data incidents; design corrective action plans (e.g., retraining models, adjusting data sources).

Lifecycle Management

- **Deployment Phase:** Use pilot programs or sandbox environments for high-risk AI tools before full-scale rollout.
- **Post-Deployment:** Schedule periodic model recalibration or re-validation to maintain performance and fairness, especially as patient demographics or data sources change (International Organization for Standardization, 2023).

Ongoing Communication & Reporting

- Provide **regular status updates** to governance committees on system performance, incidents, and risk levels.
- Maintain **dashboards** for real-time analytics on model usage, accuracy, and compliance metrics (National Institute of Standards and Technology, 2024; National Institute of Standards and Technology, 2024).

The Framework

Function 5: Continuous Improvement

Internal Audits	External Audits	Performance Assessment	Reporting & Continuous Improvement
• Scope & Frequency: Perform quarterly or semi-annual reviews of AI systems handling ePHI (U.S. Department of Health and Human Services Office for Civil Rights, 2013). • Assessment Areas: Check data privacy controls, access logs, model performance metrics, and adherence to organizational SOPs. • Remediation Tracking: Document audit findings and ensure timely resolution (National Institute of Standards and Technology, 2024).	• Engage independent auditors to assess compliance with HIPAA/HITECH [6] and other relevant frameworks (International Organization for Standardization, 2023; National Institute of Standards and Technology, 2024). • Encourage vendor audits to verify that third-party AI solutions meet contractual and regulatory obligations.	• Evaluate clinical accuracy (e.g., sensitivity, specificity) for AI diagnostics, as well as operational KPIs (efficiency gains, cost reductions). • Monitor AI fairness: Use demographic checks to detect disparities in care outcomes (National Institute of Standards and Technology, 2020; National Institute of Standards and Technology, 2024).	• Final Audit Reports: Submit to oversight boards and, if applicable, to regulators (OCR, state health agencies). • Feed audit insights back into Governance & Oversight and Management functions for iterative risk mitigation.

Impact Analysis

Sample Risk Matrix

Short-Term (0-24 months)		Risk Category	Probability	Impact	Mitigation Effectiveness	Residual Risk
• Security Enhancement: Reduction in patient data vulnerabilities through standardized encryption protocols and access controls • Operational Efficiency: Decrease in compliance-related administrative burden through clear AI governance guidelines • Incident Management: 72-hour average breach detection time • Financial Impact: More savings per healthcare organization in breach-related costs		Data Breaches	Medium (0.4)	High (0.8)	75% reduction via monitoring and MFA	Low (0.1)
		Algorithmic Bias	High (0.7)	High (0.8)	80% reduction via audits and diverse datasets	Low (0.11)
Long-Term Benefits (2-5 years)		Over-Regulation	Medium (0.5)	Medium (0.5)	60% reduction via phased implementation and iterative reviews	Low (0.1)
• Trust Metrics: Increased patient confidence rating in AI healthcare solutions • Innovation Indicators: Increase in compliant AI healthcare solutions entering market annually • Cross-Border Operations: Reduction in international data transfer complications through harmonized standards • Market Growth: Projected increase in compliant AI healthcare market valuation by Year 5		Implementation Failure	Low (0.3)	High (0.9)	85% reduction via governance oversight and milestone tracking	Very Low (0.04)

References

- Department of Health and Human Services Office for Civil Rights. (2013). HIPAA Administrative Simplification Regulation Text. Retrieved from Department of Health and Human Services Office for Civil Rights: <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>
- Accenture. (2022). Accenture Digital Health Technology Vision 2022. Retrieved April 2025, from Accenture: <https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-178/accenture-digital-health-technology-vision-2022.pdf#zoom=40>
- Ferrara, M., Bertozzi, G., Fazio, N. D., Aquila, I., Fazio, A. D., Maiese, A., . . . Russa, R. L. (2024, February 27). Risk Management and Patient Safety in the Artificial Intelligence Era: A Systematic Review. *Healthcare*, 12(5).
- HITRUST. (2023, November 21). Navigating the Security Risks of AI in Healthcare. Retrieved April 2025, from HITRUST: <https://hitrustalliance.net/blog/navigating-the-security-risks-of-ai-in-healthcare>
- International Organization for Standardization. (2023, December 18). ISO/IEC 42001:2023 Artificial Intelligence Management Systems. Retrieved from International Organization for Standardization: <https://www.iso.org/standard/81230.html>
- National Institute of Standards and Technology. (2020, January 16). Privacy Framework. Retrieved from National Institute of Standards and Technology: <https://www.nist.gov/privacy-framework/privacy-framework>
- National Institute of Standards and Technology. (2023, January). AI Risk Management Framework. Retrieved from National Institute of Standards and Technology: <https://www.nist.gov/itl/ai-risk-management-framework>
- National Institute of Standards and Technology. (2024, February 26). Cybersecurity Framework. Retrieved from National Institute of Standards and Technology: <https://www.nist.gov/cyberframework>
- National Institute of Standards and Technology. (2024, July). NIST Trustworthy and Responsible AI NIST AI 600-1 Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Retrieved from National Institute of Standards and Technology: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
- Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019, October 25). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447-453.
- Palaniappan, K., Lin, E. Y., & Vogel, S. (2024, February 28). Global Regulatory Frameworks for the Use of Artificial Intelligence (AI) in the Healthcare Services Sector. *Healthcare*, 12(5).
- Ranjbar, A., Mork, E. W., Ravn, J., Brøgger, H., Myrseth, P., Østrem, H. P., & Hallock, H. (2024, April 10). Managing Risk and Quality of AI in Healthcare: Are Hospitals Ready for Implementation? *Managing Risk and Quality of AI in Healthcare: Are Hospitals Ready for Implementation?*, 17, 877-882.
- The HIPAA Journal. (n.d.). The HIPAA Journal. Retrieved from The HIPAA Journal: <https://www.hipaajournal.com>
- U.S. Department of Health and Human Services. (2009). HITECH Act Enforcement Interim Final Rule. Retrieved 2025, from U.S. Department of Health and Human Services: <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>
- U.S. Department of Health and Human Services Office for Civil Rights. (2013). Cases Currently Under Investigation. Retrieved April 2025, from U.S. Department of Health and Human Services Office for Civil Rights: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf